REDUNDANT STRUCTURES

for FAULT-TOLERANT CONTROL

A thesis submitted to the

Department of Electrical and Computer Engineering
College of Engineering
Division of Graduate Studies and Research
of the University of Cincinnati

in partial fulfillment of the requirements
for the degree of

MASTER OF SCIENCE

December, 1991

Victor J. Hunt

B.S. Electrical Engineering
University of Cincinnati, 1988

REPORT DOCUMENTATION PAGE

AFRL-SR-BL-TR-98-

0733

1. AGENCY USE ONLY (Leave Blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	December, 1991	Final

4. TITLE AND SUBTITLE
Redundant Structures for Fault-Tolerant Control

5. FUNDING NUMBERS

6. AUTHORS
Victor J. Hunt

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
University of Cincinnati

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
AFOSR/NI
4040 Fairfax Dr, Suite 500
Arlington, VA 22203-1613

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION AVAILABILITY STATEMENT
Approved for Public Release

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*
See Attachment

14. SUBJECT TERMS

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

ABSTRACT

An increasing national priority on quality in product design and manufacturing requires new understanding to achieve significant advancement. Fault-tolerant control, a discipline capable of high-level decision making and task execution, is a necessary component for ensuring system reliability in the hierarchy of intelligent control systems. In contrast with current research, redundant control structures provide real-time fault tolerance and error accountability for systems in an untended manufacturing environment without the use of a process model. Fault detection and isolation (FDI) is optimized with respect to a risk or cost function equivalent to the probability of decision error and is generalized to account for both positive and negative faults within any controller. The resultant test compares a significant statistic to a derived threshold which is adjusted over the mission to reflect any change in the reliability of the control structure. The performance of the FDI scheme is found to be proportional to the failure signal-to-noise ratio. The effect of multiple faults on the probability of decision error is found to be negligible, assuming an uniform fault distribution. Analysis of these redundant structures and their associated FDI and reconfiguration schemes emphasizes a probabilistic set of system states which represents all a priori uncertainty inherent within the control system. Information theory defines entropy as a logarithmic measure of system/decision uncertainty. This allows for a comparison of the effective system performance of redundant structures. The optimal redundant structure for fault-tolerance is reached by utilizing a highly reliable control structure at the greatest level of redundancy while maintaining near-perfect FDI at all levels of operation. This allows maximizing the information rate of the discrete FDI decision scheme while minimizing the error variance of the controlled parameter. Further, the average mission or period of working operation is increased due to successive stages of reduced operation.

Acknowledgements

In any endeavor, there are those whose contributions cannot be overlooked

and without whom the work would not be possible.

I would like to thank

Dr. Patrick Garrett

Dr. Bruce Walker

Dr. Steven LeClair

and, Mr. Jeff Heyob

for their guidance, support, and friendship.

I would also thank my parents and family for their love and encouragement.

Most of all I thank my friend for life, Tracy.

This work was supported by an Air Force Lab Fellowship
under the direction of Dr. Warren Peele, SCEEE
11th & Massachusetts Ave, St. Cloud, FL 34769

TABLE OF CONTENTS

Chapter 1: The Problem, Method of Approach, and Results

1.1. The Challenge for Quality

An increasing national priority on quality in product design and manufacturing requires new understanding to achieve significant advancement. As real-time, computer-based measurement and actuation systems have increased in complexity, human capabilities to conceptualize such systems with mathematical models have been challenged. The IEEE Control Systems Society and the National Science Foundation (NSF) invited fifty-two eminent contributors in the field of control to a workshop at the University of Santa Clara in September, 1986. Their perspectives on important research areas, documented in "Challenges to Control: A Collective View" by editor A. H. Levis, included:

> Due to the often unrealistic assumptions that the mathematical model of the system be completely known and that the model have the form of linear differential (or difference) equations . . . control theorists are now challenged to expand their horizons and to extend their concepts and methods to be applicable to incompletely modeled systems . . . [Levis]

Indeed, current engineering strategies show widespread traditional use of empirically designed manufacturing elements, described in terms of qualitative domain knowledge as opposed to quantitative modelling efforts. [Bobrow] Processes which necessitate these highly complex representations can benefit from equally complex self-organizing (i.e. intelligent) control structures to accommodate incomplete a priori knowledge and reducible uncertainties. This "complex process - complex controller" paradigm constitutes the most advanced automatic control presently realizable, and provides the basis for a productive research effort to achieve new levels of performance, and hence quality, in manufacturing enterprises. [Saridis]

Fault-tolerant control, a discipline capable of high-level decision making and task execution, is a necessary component for ensuring system reliability in the hierarchy of intelligent control systems. [Saridis] Coverage is the property of a system which defines its ability to tolerate failures of a specified subset or percentage of its components (i.e. the degree of its fault tolerance). Fault-tolerant applications that require the most efficient coverage of any failures at all times, within given limitations on hardware and knowledge, dictate the use of fault detection and isolation (FDI) schemes to properly reconfigure the system for continued operation with a minimal loss in performance. Levis writes:

> A more general class of control systems which adapt to significant changes in their environment is ... fault-tolerant control systems. In this class of problems we admit that one or more key components of the physical feedback system will fail and that this failure can have significant impact on stability or performance. The idea is to design the control system so as to retain stability and lose performance in a gracefully degraded manner. It may be necessary to reconfigure the control system following the detection of such failures. For example, a real-time decision will have to be made on whether we should ... accept some performance degradation or ... concentrate on maintaining stability and perhaps - after the transients have died out - reconfigure again to achieve optimal performance. A challenging problem for control theory is to take into account advances in computer technology and to stimulate the development of real-time and concurrent systems which allow the implementation of such control strategies in hardware form. [Levis]

This challenge is taken up in the following thesis on the implementation and analysis of fault-tolerant control with redundant control structures.

In contrast with current fault-tolerant control schemes, the dual-difference redundant structure (DDRS) and triple redundant structure (TRS) provide real-time fault

environment without the use of a process model. A major concern during the control of any system or process is the level of confidence associated with the controlled parameters. In a paper on the fundamental issues and architecture for autonomous control systems, Antsaklis also determined the necessity of fault-tolerant control in an environment of significant uncertainty:

> There must be certain features inherent in the autonomous system design. In addition to supervising and tuning the control algorithm, the autonomous controller must also provide a high degree of tolerance to failures. Design features should prevent failures that would jeopardize the overall ... mission goals or safety. This implies that the controller should have self-test capability ... , tolerance of transient errors, adjustable fault detection thresholds, reversible state changes, and protection from invalid external commands. To achieve this, high level decision making techniques for reasoning under uncertainty and taking actions must be utilized. [Antsaklis]

The fault-tolerant control structures presented in this thesis are designed to take advantage of the benefits of redundancy while incorporating these and other design features. These redundant structures represent the base level in a possible hierarchy of system fault detection and diagnostic schemes. [Saridis, Antsaklis] Upon validation of the control structure by FDI algorithms, confidence can be placed in the controlled parameter within the derived accuracy. This allows a solid base upon which to build further reasoning about the process or system. With the empirical knowledge provided, the host system can monitor the process, infer its current state via process models, and reason about future control needs. This concept highlights the distinction from current fault-tolerant schemes which utilize an explicit process model as the very foundation of the control hierarchy and have been found to be highly sensitive to uncertainty or error within the process model. [Emami-Naeini, Horak]

The FDI algorithms designed for the redundant control structures are based upon a mapping from the observable or measurable space of the control system to a hypothesis/decision space and therefore implies a decision-making process. Levis refers to this form of hypothesis testing as a "hybrid model approach" incorporating both higher discrete levels of information and the continuous data received at the process level.

> Multiple model hypothesis testing is a very important process in symbolic reasoning. In such problems we have a discrete set of alternative interpretations of data, we have models for each, and we have optimal processors for each that allow us to produce statistics that form the basis for efficient and rational assessment of which alternative is most likely to be correct. ... This hybrid model approach provides a framework in which it is possible to think about fusing all types of knowledge and information. It also very naturally reduces data and knowledge to statistics as the basis for higher-level reasoning and is well set up for parallel processing. ... the modelling of (this) uncertainty is to be "structured" so as to exploit all relevant a priori information about the plant to be controlled, including not only numerical, but also qualitative and linguistic descriptions. [Levis]

Analysis of these redundant structures and their associated FDI and reconfiguration schemes emphasizes a probabilistic set of system states which represents all a priori uncertainty inherent within the control system. This status information, presented to the host system, provides a confidence metric with each controlled parameter and thus facilitates qualitative reasoning about the process for goal-oriented control purposes [Garrett, Matejka, Fox]. For example, in a qualitative control system which can select among alternative control actions during a specific process instance to achieve process goals, the availability of this controller status information can meaningfully influence this choice by quantifying the confidence associated with each measured variable. Hence, the hierarchy of intelligent controllers combines local, low-level observation and broader, higher-level reasoning and planning in order to ensure continuous and efficient system performance and knowledge.

Entropy provides the structure which Levis sought in a model of uncertainty ... a structure in which different knowledge sources can be represented, combined, and compared. The concept of entropy has a rich history that defies disciplinary boundaries in its application. Information theory defines entropy as a logarithmic measure of the randomness or 'choice' involved in an event or the prior uncertainty of the outcome of an experiment. Shannon's celebrated paper on the "Mathematical Theory of Communication" in the Bell System Technical Journal, 1948, is generally considered to be the first detailed exposition on information theory. [Shannon] Saridis and Valavanis use entropy as an unified quantification of disorder in each of three levels (i.e. execution, coordination, and management) of a heirarchical system based on the principle of "increasing intelligence with decreasing precision". In an intelligent controller, the control action that will decrease the entropy of the system is initiated. [Valavanis] Stephanou found that entropy provides a quantitative criterion for measuring the effectiveness of a consensus obtained from the pooling of evidence from independent knowledge sources. This focusing of knowledge allows a subsequent reduction in an experiment's uncertainty or entropy. [Stephanou] In this thesis, this metric of uncertainty allows for comparisons of the effective system performance for different redundant structures. For example, system entropy is found to decrease with each level of redundancy when a near-optimal FDI scheme is employed. In addition, the benefits of active redundancy over passive techniques such as majority-voting is clearly observed. This widespread application of entropy attests to its fundamental nature and allows for linkage into a more comprehensive system representation of uncertainty by incorporation of other system entropies.

1.2. Method of Approach

In Chapter 2, an analysis of the typical control structure by Garrett describes each functional component of the system and provides a tabular form for itemizing, quantizing, and minimizing worst-case errors of an average, random, or systematic nature. [Garrett] This error budget presents all error sources and their bounds in a standard format to allow comparison and combination of all system errors. The result is a stationary, Gaussian error function of minimal mean and variance conditioned on the reliable performance of the control structure. This probability density function defines the uncertainty of the control structure at any given point in time of its operation. However, we are also uncertain as to whether the control structure is operating properly at this stage in its lifetime or mission. The following chapter reviews reliability theory and proposes a failure rate budget (the conceptual equivalent to the error budget) to account for all sources of failure within the control structure. Reliability is represented by a maximized exponential density function of time. These models provide a complete concept of all a priori knowledge of the control structure. It is found in Chapter 5 that these functions conform to Jaynes' method of maximum entropy where a chosen model remains minimally prejudiced with respect to any missing information. Thus, our error and reliability models exhibit a dualism in their origination and application. Further, these models can be optimized with respect to each application based on the give-and-take between the costs of various sources included in the error and failure rate budgets.

In Chapter 3, we also find that redundancy allows further improvement of the control structure's error and reliability. For example, the deviation in the error function of the control signal is reduced through the averaging of the redundant outputs, owing to the essentially uncorrelated error contributions of each structure's elements. This reduction in error variance is shown to be optimal with respect to redundant hardware for two structures. Analysis of redundant structures shows additional benefits in improved

reliability occurring with each level of redundancy. Each additional structure in a redundant configuration provides an order of magnitude improvement in the reliability of the configuration during short term missions or earlier periods of extended operation. However, these benefits are only possible under the unlikely assumption of perfect fault coverage and, without such ideal conditions, are achieved at the cost of increased entropy or uncertainty with each level of redundancy (Chapter 5). An attempt to recoup these losses via fault detection and isolation techniques is presented in Chapter 4.

In Chapter 4, the dual-difference redundant structure (DDRS) and triple redundant structure (TRS) are designed to provide fault-tolerant control (i.e. fault detection, isolation, and reconfiguration) to the extent of their capabilities. Active redundancy achieves greater fault coverage than the masking techniques of passive redundancy (e.g. TMR or NMR) in that fault occurrences are detected and not merely screened. The dual-difference redundant structure provides quick and efficient front-end fault detection with a simple difference test, yet fault isolation is only possible to the extent which the simplex fault detection schemes provide fault coverage. The triple redundant structure, however, provides both efficient fault detection and isolation with a more complex FDI scheme. Additionally, limit and rate checking will detect extreme bias and noise conditions which comprise the majority of spontaneous or transient faults. Reconfiguration consists of a graceful and recoverable reorganization of the system to a structure of lesser redundancy and reduced performance. Hence, each redundant control structure is a subset of all structures of greater redundancy. For example, the TRS is reconfigured to the DDRS upon fault detection with the two remaining valid controllers. In this manner, fault-tolerant control is achieved. However, any problems occurring within the process or to the signal outside of the control structure can not be considered a fault. Deviations of the measured parameter from expected values due to these problems will be transparent to the FDI scheme and must be detected by the host computer at system level.

The fault detection and isolation (FDI) scheme assumes a classical, M-ary hypothesis test with a fixed, singular data sample. Thus, there are M possible alternatives or event-hypothesis pairings each time a decision must be made. With any decision-making process comes the possibility of decision errors; in this case, there is an inherent give-and-take between the two decision errors of false alarms and missed detections. With any FDI scheme, it is found that the probability of these decision errors is inversely proportional to the failure signal-to-noise ratio (SNR). This analysis is concerned with the worst-case magnitude of f (f_{min}) which is the smallest fault (and, thus, the hardest to detect) of accountable cost for the current application. It is further generalized to account for both positive and negative faults within any controller. A second concern of decision error is the possible missed detection of certain multiple faults which are hidden from the FDI scheme. For example, the difference test is insensitive to a dual fault where a fault of approximately equal amplitude occurs on both controllers. This analysis assumed a uniform fault distribution across the space of all possible faults and found the effect of multiple faults on the probability of decision error to be negligible. The resultant set of system states and their associated probabilities is determined from a decision tree for each redundant structure based on its FDI and reconfiguration schemes.

Several fault detection and isolation schemes are examined for each redundant structure. The FDI scheme can be optimized by using a generalized likelihood ratio test (GLRT) which is based on a degenerated Bayes criterion. This analysis utilizes the special cost assignment where correct decisions incur no penalty and incorrect decisions incur the same penalty. With this cost assignment, risk is equivalent to the probability of decision error. The likelihood ratio is determined directly from the ratio of the marginal or conditional densities of the parameter or parity vector under either event. Another possible FDI scheme is based upon the classical Neyman-Pearson criterion of radar detection theory. Here, the conditional probability of false alarms P_{FA} is constrained to remain less

than some arbitrarily small value α, known as the level or significance level of the test, and then the conditional probability of fault detection P_D is maximized to some value $(1-\beta)$, known as the power of the test. The resultant test for either FDI scheme compares a significant statistic (e.g. the radius or absolute difference) to a derived threshold and is thus generalized in order to account for a fault in any controller. This threshold is held constant by the Neyman-Pearson criterion and is completely defined upon choosing the level of the test (α). For the Bayes criterion, the threshold is varied according to the prior event probabilities of the control structure in order to minimize the probability of decision error. For example, the threshold is originally made quite large compared to the fault magnitude while the probability of normal operation is high and is subsequently pulled closer to the origin as the probability of a structure fault becomes predominant.

In Chapter 5, we analyze all relevant a priori uncertainty or entropy within the control system. The minimized Gaussian error function and the maximized exponential reliability function provide a complete concept of all a priori knowledge of the control structure. The marginal or conditional probabilities of the FDI schemes describe the performance statistics associated with the redundant structure. The resultant set of system states and their associated probabilities, as illustrated by the decision tree, represents all a priori uncertainty in the control system. Information theory defines entropy as a logarithmic measure of the randomness or 'choice' involved in an event or the prior uncertainty of the outcome of an experiment. This metric of uncertainty allows for comparisons of the effective system performance for different redundant structures.

1.3. Results and Conclusions

1. This thesis concerns the implementation and analysis of redundant structures in fault-tolerant control. Complex, intelligent control structures are sought which: provide robust, optimized fault tolerance; can be implemented efficiently upon any process; and do not require a process or signal model. These structures can be utilized in a broad range of applications and define a unifying base for the hierarchical architecture of autonomous control.

2. In contrast with current fault-tolerant control schemes, the dual-difference redundant structure (DDRS) and triple redundant structure (TRS) provide real-time fault tolerance and error accountability for sensor systems in an untended manufacturing environment without the use of a process model. The DDRS provides quick and efficient front-end fault detection with a simple difference test, yet fault isolation is only possible to the extent which the simplex fault detection schemes provide fault coverage. The TRS, however, provides both efficient fault detection and isolation with a more complex FDI scheme. Reconfiguration consists of a graceful and recoverable reorganization of the system to a structure of lesser redundancy and reduced performance. In this manner, fault-tolerant control is achieved.

3. Full redundancy of the control structure is not always feasible. The additional hardware requires more expense and working volume than can sometimes be afforded. In fact, space limitations and expense are two major reasons why redundant structure configurations are avoided and research has shifted to analytical redundancy.

4. Fault detection and isolation (FDI) is optimized with respect to a risk or cost function equivalent to the probability of decision error. The FDI scheme is generalized to account for both positive and negative faults within any controller. The resultant test compares a significant statistic to a derived threshold which is adjusted over the mission to reflect any change in the reliability of the control structure.

5. The performance of the FDI scheme is found to be proportional to the failure signal-to-noise ratio. The effect of multiple faults on the probability of decision error is negligible, assuming an uniform fault distribution.

6. Limit and rate checking will detect extreme bias and noise conditions which comprise the majority of spontaneous or transient faults. Reconfiguration consists of removing the faulty controller from the output estimation scheme yet still including it as a voter in the FDI scheme. The faulty controller is simply returned to valid status upon a successful test. This reconfiguration scheme allows recovery from false alarms and transient faults and maintains the independence between successive tests over the mission.

7. The minimized Gaussian error function and the maximized exponential reliability function provide a complete concept of all a priori knowledge of the control structure. The marginal or conditional probabilities of the FDI schemes describe the performance statistics associated with the redundant structure. The resultant set of system states and their associated probabilities, as illustrated by decision tree, represents all a priori knowledge of the redundant structure.

8. Entropy provides a logarithmic measure of system/decision uncertainty. This metric allows for a comparison of the effective system performance of redundant structures. Further, the widespread application of entropy attests to its fundamental nature and allows for linkage into a more comprehensive system representation of uncertainty by incorporation of other system entropies.

9. The optimal redundant structure for fault-tolerance is reached by utilizing a highly reliable control structure at the greatest level of redundancy while maintaining near-perfect FDI at all levels of operation. This allows maximizing the information rate of the discrete FDI decision scheme while minimizing the error variance of the controlled parameter. Further, the average mission or period of working operation is increased due to successive stages of reduced operation.

10. For a system with zero shutdown cost and high false alarm cost, the general performance of a redundant structure is dependent upon the quality of the tests and proper design of the decision scheme. Results indicate the need to switch the FDI decision scheme for different stages of the mission in all but the most perfect case. Any detection schemes of poor or worse quality are generally not utilized. However, a redundant structure with shutdown capability must incorporate at least one quality test in order to improve upon single structure performance.

Novel contributions of this thesis include:

* Analysis of the sensitivity of the FDI scheme to multiple faults.

* A more optimal fault detection scheme for triple redundant structures.

* Analysis and comparison of the uncertainty within redundant structures.

Chapter 2: Error Analysis of the Control Structure

Computer applications have been widespread since the first real-time minicomputer implementation for process measurement and control in 1958. Progress has been especially rapid since the introduction of the microcomputer. Successful integration of the computer system within the process control loop relies directly upon accurate input/output (I/O) interfacing. Yet many current designs of data acquisition and control actuation are based on traditional "cookbook" methods. Economic and performance requirements demand improved error accountability and reduced product variability through a comprehensive quantitative analysis of the interface from sensors to actuators. This mathematical model-based approach provides a definitive framework on which to build intelligent control. A typical control structure is presented in Figure 2.1. This structure can represent either the inner-loop digital control of the process (Figure 2.2) or an outer loop observer/planner to reason qualitatively about the system (Figure 2.3).

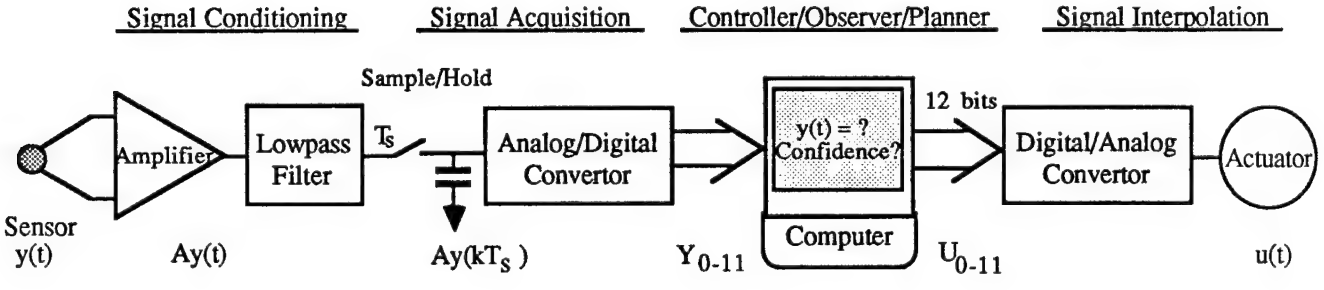


Figure 2.1 Typical Control Structure

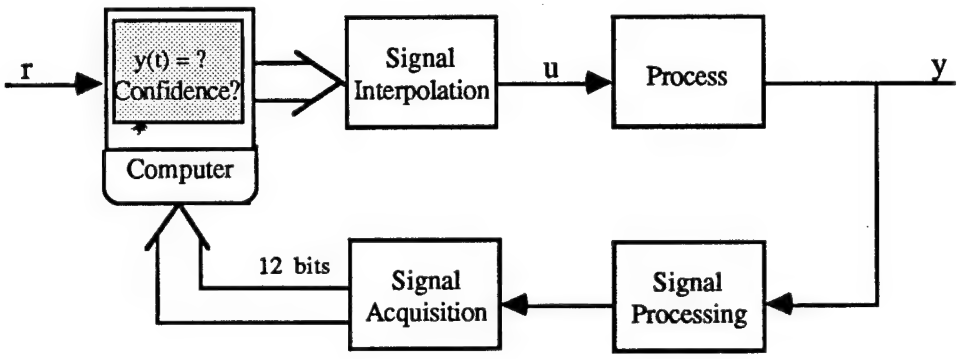


Figure 2.2 Inner Loop Control

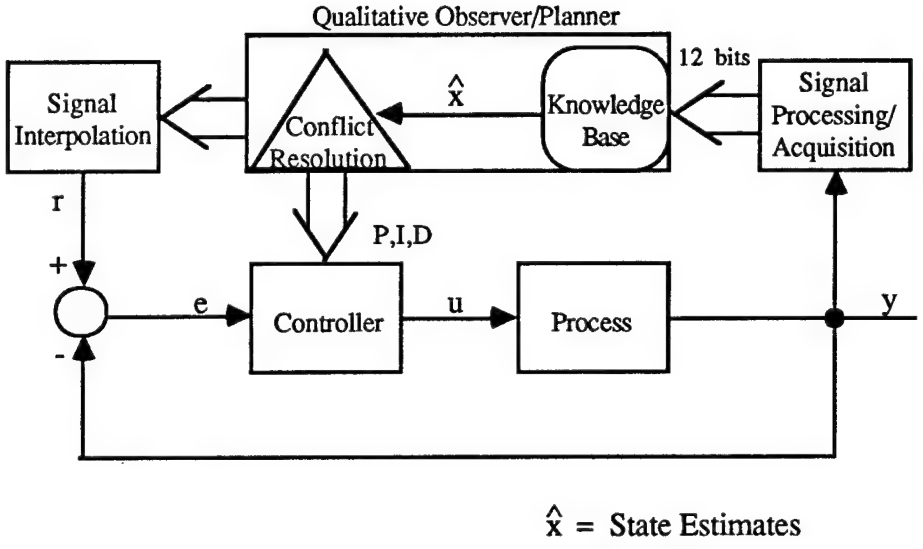


Figure 2.3 Outer Loop Observer/Planner

An analysis by Garrett of the typical control structure describes each functional component of the system and provides a tabular form for itemizing worst-case errors. [Garrett] This error budget presents all error sources and their bounds in a standard format to allow comparison and combination of all system errors. Thorman's analysis of an existing control structure is presented in Figure 2.4 (see also Appendix A) as an example of an error budget. [Thorman] Three error characteristics are encountered in practice: average, systematic, and random. Average error is the mean value of parameter variation, as represented by hardware and sampling errors. Systematic errors are those which vary as a function of operating conditions, such as device temperature drift and intersample error. Random errors are parameter variations possessing a probability density function (pdf), such as signal quality and device/system noises. All values are given in terms of percent of full scale measurement (%FS) in order to provide a common scale for comparisons. The Central Limit Theorem dictates that the pdf of random, uncorrelated errors is approximated by a normal or Gaussian distribution over a large (infinite) number of samples. The characteristic bell-shaped curve, as depicted in Figure 2.5, is completely defined by its mean (μ = summation of all average errors) and standard deviation (σ = root-sum-square of all random and systemic errors). This orthogonal summation of component Gaussian distributions is due to the independent or uncorrelated nature of the error sources (the RSS cross-product terms are zero). [Papoulis, Peebles] Error terms may now be quantified and combined to provide an overall measure (or window) of performance for the current design and environment of the control structure. Equation 2.1 presents the conditional error density function for the analyzed control structure given that the structure is reliable or functioning properly (Section 3.2). This window of performance is the basis for our fault detection scheme discussed in Chapter 4.

System Element	Error (%FS)
Sensor linearization	0.0111
Cold junction compensation	0.0222
Input RC filter	0.0001
Signal quality	0.2370
OP-07 amplifier	0.0370
CMOS multiplexer	0.0110
A/D converter	0.0066
Intersample	0.0319
Sinc	0.0150
Aliasing	0.2205
Mean value (μ)	0.0484
RSS value (σ)	0.3276
Existing measurement error bound	0.3760 %FS (6.77 °C)

Figure 2.4 Example Error Analysis for a Control Structure

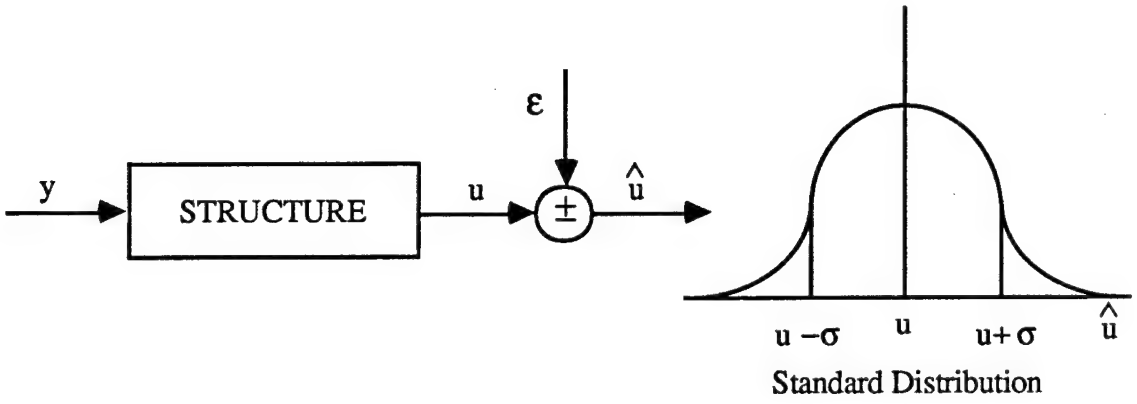


Figure 2.5 Control Structure Error PDF

$$\mathcal{E}(x \mid \text{Reliable Structure}) = \text{Gaussian}\left(\mu = \sum \overline{\varepsilon_{\text{average}}},\ \sigma = \sqrt{\sum \varepsilon^2_{\text{random}} + \sum \varepsilon^2_{\text{systematic}}}\right)$$

$$= \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right)$$

(Equation 2.1)

Our attention now turns to achieving the design with the lowest error bound and, therefore, the best performance. The most efficient estimator of the control signal has the smallest variance (σ^2) in the error. Error variance can be minimized through proper use and configuration of each system parameter and component. The following sections are devoted to the understanding, quantization, and minimization of the major error sources within the control structure. Our end result is a stationary Gaussian error function with mean μ and minimal variance σ^2 associated with the given control structure and conditioned on its normal operation (i.e. no faults).

2.1. Average Filter Error

Standard signal conditioning practice dictates the need for a lowpass filter whose cutoff frequency is placed at the highest frequency of interest in the system. Requirements for signal bandlimiting in data acquisition and conversion systems include signal quality upgrading (section 2.2) and aliasing prevention (section 2.3.3). However, when a filter is superimposed on the measured signal, filter gain and phase deviations from the ideal result in a signal amplitude error that constitutes component error. Filter gain error is the primary source of error for both DC and sinusoidal signals because single line spectra are unaffected by filter phase nonlinearities. Laube analyzed the passband gain deviation for three common filters with reference to 0 Hz (Figure 2.6). [Laube] Most applications are best served by the 3-pole Butterworth filter which offers good stopband attenuation and 0.2%FS error for 50% spectral occupancy of the passband. Of significance is that small filter component error can be achieved, with a small sacrifice of the total filter bandwidth, by restricting signal spectral occupancy to a fraction of the filter cutoff frequency.

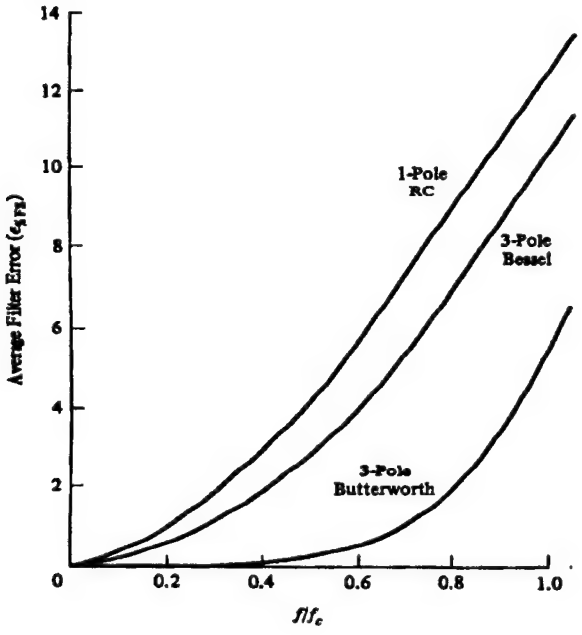


Figure 2.6 Passband Gain Deviations for Three Filters

2.2. Signal Quality

The basic signal conditioning structure of the preamplifier and filter is commonly used to reduce the interference of unwanted signals (noise). Garrett analyzed signal corruption due to random Gaussian noise or coherent sinusoidal interference. [Garrett] The signal-to-noise ratio (SNR) is a dimensionless ratio of signal power to noise power which provides a measure of the interference. Equations 2.2 - 2.5 allow determination of the filter output SNR by accounting for the effects of signal conditioning and either random or coherent noise on the measured input SNR. SNR will be expressed as the squared rms ratio of full scale signal amplitude to maximum noise amplitude (assuming equal resistance for both). In Equation 2.3, the resistances to the signal and noise sources within the amplifier are represented by the differential and common-mode impedances, respectfully. The amplifier's common-mode-rejection-ratio (CMRR) is squared in order to convert its ratio of differential to common-mode voltage gains into a power ratio. The filter's efficiency (k) represents its approximation to ideal matched-filter signal conditioning with respect to random interference (Equation 2.4) and any coherent sinusoidal interference (f_{coh}) beyond the filter's cutoff frequency (f_c) will be greatly attenuated (Equation 2.5).

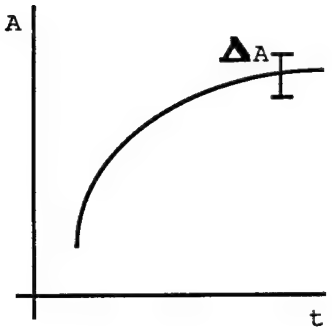
$$SNR_{input} = \left[\frac{V_{diff}}{V_{cm}}\right]^2 \quad \frac{dc}{dc} \text{ or } \frac{rms}{rms} \qquad \text{(Equation 2.2)}$$

$$SNR_{amp} = SNR_{input} * CMRR^2 * \frac{R_{cm}}{R_{diff}} \qquad \text{(Equation 2.3)}$$

$$\text{Filter } SNR_{random} = SNR_{amp} * k * \frac{f_{hi}}{f_c} \qquad \text{(Equation 2.4)}$$

$$\text{Filter } SNR_{coherent} = SNR_{amp} * \left[1 + \left(\frac{f_{coh}}{f_c}\right)^{2n}\right] \qquad \text{(Equation 2.5)}$$

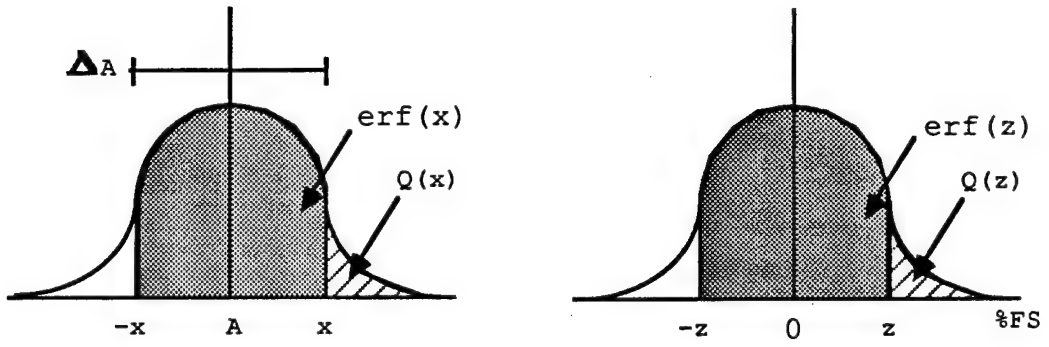
The filter output SNR is used directly in determining the signal quality (equations 2.6,2.7). The square root of the SNR is the ratio of full scale signal-to-noise amplitudes. For coherent interference, signal error (%FS) or the ratio of full scale noise-to-signal amplitudes is easily found from the inverse of the SNR square root (Equation 2.6).



$$\varepsilon_{coh} = \frac{\Delta A}{A} 100\% = \frac{V_{coh}}{V_{FS}} 100\%$$

$$= \frac{100\%FS}{\sqrt{SNR_{coherent}}} \qquad \text{(Equation 2.6)}$$

For random Gaussian noise (Figure 2.7), the signal error pdf must be evaluated at the noise region (ΔA) centered about the true signal amplitude (A) in order to achieve 68% confidence (i.e. $\pm$ one standard deviation) in accordance with our signal error distribution. The erf function approximates the area (probability) under the standard Gaussian curve (zero mean and unit variance) within some region centered about the mean. [Schwartz] Transformation to the standard distribution (x transformed to z) requires normalization of the delta region by full scale conditions (the SNR square root). Here, the erf function is given in terms of the Q function which represents, in a tabular form, the area under the curve for all values greater than z. [Shanmugam] When erf(z) is evaluated at 68% probability, the error contribution due to random interference can be determined (Equation 2.7).



Standard Distribution

$$x = A \pm \frac{\Delta A}{2} \longrightarrow z = \pm \frac{\Delta A}{2A} \frac{V_{FS}}{V_{random}} = \frac{\varepsilon_{random}}{200\%FS} \sqrt{SNR_{random}}$$

(transformation to Standard Distribution)

$$erf(z) = 1 - 2Q(z\sqrt{2}) = 68\%;$$

$$z = \frac{1}{\sqrt{2}} \qquad \text{(from Q Table: Q(1) = 16\%)}$$

$$\varepsilon_{random} = \frac{100\%FS\sqrt{2}}{\sqrt{SNR_{random}}} \qquad \text{(Equation 2.7)}$$

Figure 2.7 Random Gaussian Interference

2.3. Sampled Data

Digital transmission of analog signals is possible by virtue of the sampling theorem which tells us that an analog signal can be reproduced from an appropriately spaced set of its samples. True reproduction of the signal requires a number of ideal conditions: bandlimited, continuous signal; infinite, impulse sampling; and ideal, lowpass interpolation. Most physical signals may be considered bandlimited due to the small amplitude of high-frequency components. Practical application and system stability requirements enforce sampling of finite rate and pulse width. The ideal interpolation function cannot be physically realized because its noncausal impulse response requires an output that anticipates its input. Therefore, in practice, these factors make it impossible to exactly reproduce a continuous signal from the sampled signal even if the sampling theorem is satisfied. [Kuo]

2.3.1. ZOH Amplitude or Sinc Error

Convolution of the analog signal and an instantaneous sampling function leads to a spectrum consisting of the original baseband spectrum of the signal and its replication around each of the harmonics of the sample frequency. For sample-and-hold (S/H) applications, sinc attenuation of these images occurs due to the transfer function of a zero-order-hold (ZOH). In Figure 2.8, Kuo derives the transfer function and frequency domain representation for a ZOH. [Kuo] In Figure 2.9, Garrett shows the effect of the sinc attenuation on a sampled sinusoidal signal. [Garrett] The ZOH behaves essentially as a nonideal lowpass filter, imposing signal amplitude and phase error within the bandwidth (BW). Clearly, the accuracy of the ZOH as an extrapolating device depends greatly on the sample frequency. Garrett approximates the error imposed by sinc attenuation with the average baseband amplitude error expressed in %FS departure from unity gain (Equation 2.8). [Garrett] As the sample frequency f_S approaches the spectral occupancy of the signal, the sinc error becomes more predominant.

ZOH Transfer Function

$$g_{zoh}(t) = u(t) - u(t-T) \quad \rightarrow \quad G_{zoh}(s) = \frac{1 - \exp(-Ts)}{s}$$

$$G_{zoh}(j\varpi) = \frac{\exp(-j\varpi T/2)\left[\exp(j\varpi T/2) - \exp(-j\varpi T/2)\right]}{j\varpi}$$

$$G_{zoh}(j\varpi) = \frac{2 * \sin(\varpi T/2) * \exp(-j\varpi T/2)}{\varpi} = T * \text{sinc}(\varpi/\varpi_s) * \exp(-j\varpi T/2)$$

amplitude **phase**

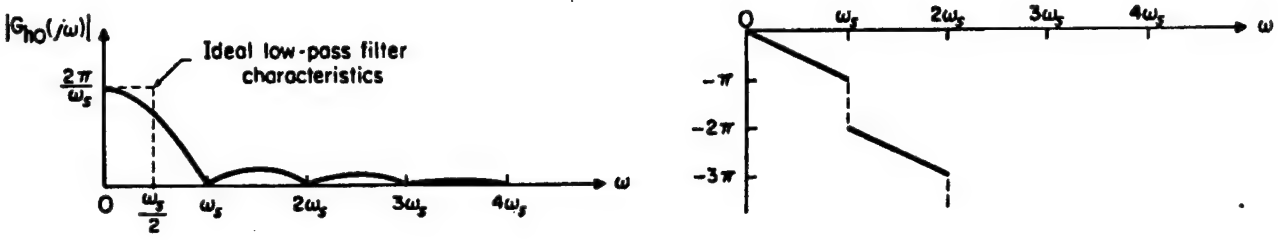


Figure 2.8 ZOH Transfer Function and Frequency Domain Representation

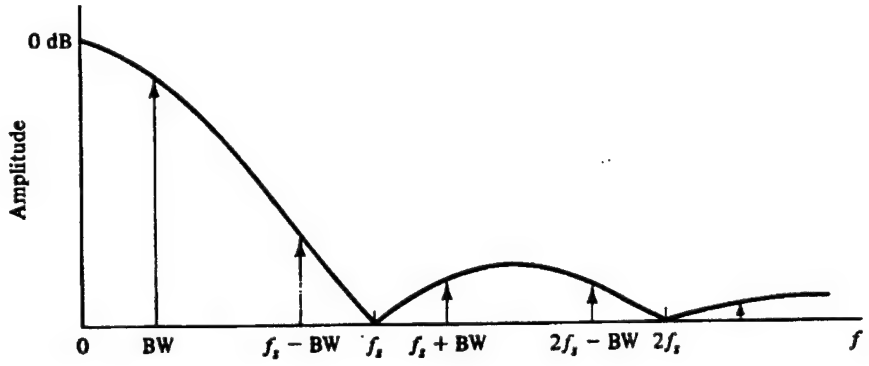


Figure 2.9 Image Spectra of Sampled Sinusoid Signal

ZOH Amplitude or Sinc Error $\quad \overline{\varepsilon_{sinc}} = 50\%FS * \left[1 - \text{sinc}\left(\frac{BW}{f_s}\right)\right]$ (Equation 2.8)

2.3.2. ZOH Phase or Intersample Error

The step-interpolation of the ZOH assumes the last sampled value is true until the next sample. Evaluation at the sample frequency of the phase term of the ZOH transfer function determines that the sampled signal exhibits an average time delay equal to half the sample period. Intersample error is the variation between the actual signal and its ZOH step-interpolated representation. In Figure 2.10, Garrett depicts the intersample error for a sampled sinusoidal signal due to the ZOH signal delay. The worst-case intersample error is found by Garrett through the following set of equations working in the time domain. Maximum peak-to-peak (pp) error is found assuming a sinusoidal signal at its maximum rate-of-change zero crossing (Equation 2.9).

$$\Delta V_{pp} = T_s * \frac{dV}{dt} \qquad \text{intersample error (pp)}$$

$$= T_s * \frac{d}{dt} V_{pk} \sin(2\pi BWt)\Big|_{t=0}$$

$$= 2\pi T_s BW V_{pk} \qquad \text{(Equation 2.9)}$$

Conversion to root-mean-square (rms) error by Equation 2.10 requires normalization by the signal's sinusoidal pp/rms factor and the intersample triangular pp/rms factor due to the error waveform in Figure 2.10.

$$\Delta V_{rms} = \frac{2\pi T_s BW V_{pk}}{2\sqrt{2} * \sqrt{3}} \qquad \text{intersample error (rms)}$$

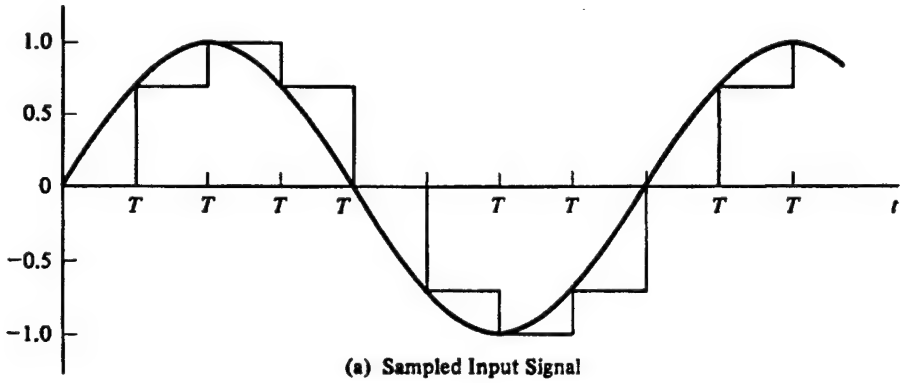
(Equation 2.10)

Finally, intersample error is provided in terms of %FS (Equation 2.11). [Garrett]

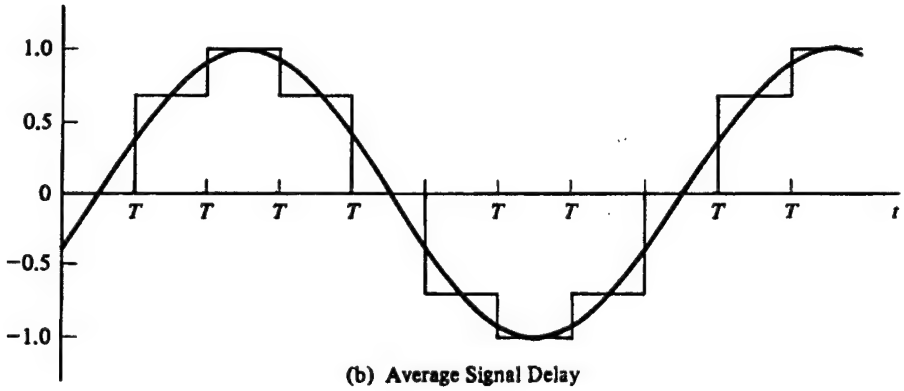
$$\varepsilon_{intersample} = \frac{\Delta V_{rms}}{V_{FS}/\sqrt{2}} \; 100\%FS$$

$$= \frac{\sqrt{2}\,\pi BW V_{pk}}{\sqrt{6}\, f_s V_{FS}} \; 100\%FS \qquad \text{(Equation 2.11)}$$

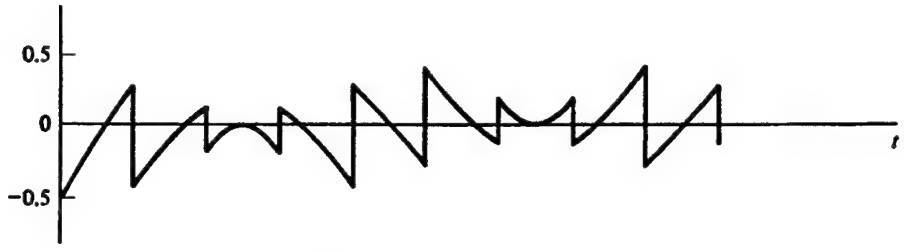
Due to the poor interpolation of the ZOH, intersample error contributes greatly to the system error budget. Its minimization requires a high fs/BW ratio or a more ideal filter (see section 2.4) to provide smoother signal recovery between samples.



(a) Sampled Input Signal



(b) Average Signal Delay



(c) Intersample Error

Figure 2.10 Intersample Error

2.3.3. Aliasing Error

By the sampling theorem, the minimum sample rate (f_S) allowing signal reconstruction is twice the signal bandwidth. Infinite sampling is ideal, but practical application and system stability enforce a finite maximum rate. As the sample frequency is reduced, samples move further apart in the time domain and images move closer in the spectrum. Signal aliasing, or spectral overlap of the baseband and its images, occurs when the folding frequency ($f_O = f_S/2$) meets the baseband. In general, sample frequency can be set high enough to readily avoid this problem of signal aliasing. [Kuo]

Of greater concern and complexity is noise aliasing. Coherent and random noise sources above the folding frequency are heterodyned within the signal baseband as a consequence of the convolution of noise and the sampling function (Figure 2.11 by Garrett). This generation of intermodulation distortion cannot be removed by later signal conditioning. The pre-sampling filter used for signal quality upgrading (Section 2.2) is our only protection against noise aliasing. The filter of order n will attenuate all unwanted noise outside its cutoff frequency in order to substantially reduce undersampling. This observation can also be made from the aliasing error equations derived by Garrett (Equations 2.12 - 2.15). [Garrett] Aliasing error due to coherent interference in the source band m (Equation 2.12) is determined from the heterodyned noise amplitude after its attenuation by the filter and the sampling sinc function.

$$\varepsilon_{\substack{coh \\ alias}} = \frac{V_{coh}\ 100\%FS}{V_{FS}} \left[1 + \left(\frac{f_{coh}}{f_c}\right)^{2n}\right]^{-1/2} \operatorname{sinc}\left(\frac{|mf_s - f_{coh}|}{f_s}\right)$$

where n = filter order
m = noise source band

(Equation 2.12)

Aliasing error due to random interference up to the amplifier's cutoff frequency (fhi) (Equation 2.15) is determined from the SNR as per Equation 2.7. The power of the aliased random noise is approximated in Equation 2.13 by summation of the attenuated noise amplitudes, squared for power, at each harmonic. Note that heterodyned random noise sources may be considered out to the first harmonic (m = 1) only due to the filter attenuation.

$$N_{alias} = \sum_{m=1}^{f_{hi}/f_s} \left(\frac{V_{random\ 100\%FS}}{V_{FS}} \right)^2 \left[1 + \left(\frac{mf_s}{f_c} \right)^{2n} \right]^{-1}$$

(Equation 2.13)

$$SNR_{\substack{random \\ alias}} = \frac{V_{FS}^2\ (rms)}{N_{alias}}$$

(Equation 2.14)

$$\varepsilon_{\substack{random \\ alias}} = \frac{100\%FS\ \sqrt{2}}{\sqrt{SNR_{\substack{random \\ alias}}}}$$

(Equation 2.15)

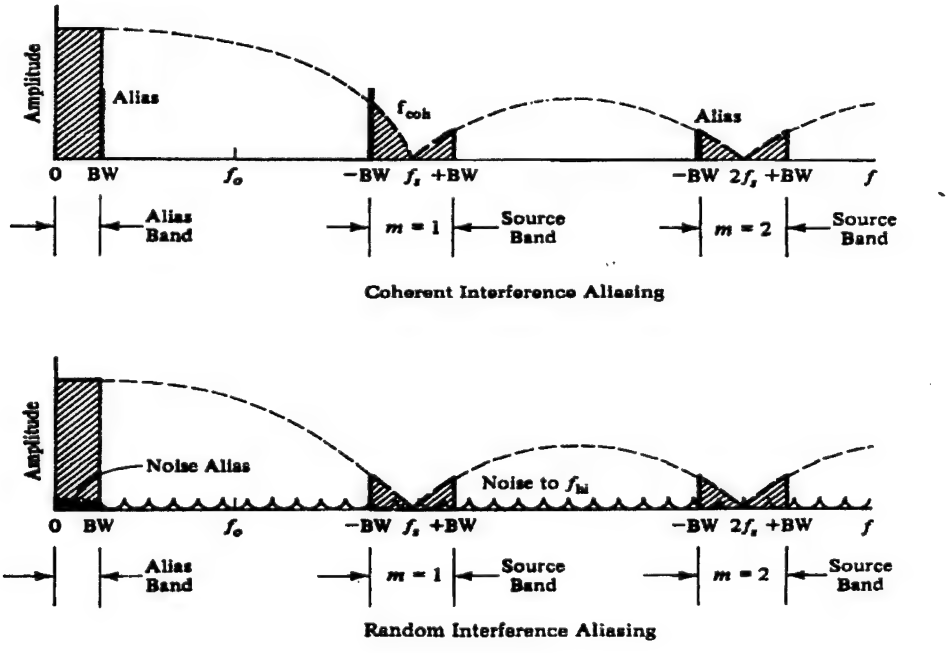


Figure 2.11 Aliasing of Coherent and Random Noise

2.4. Signal Recovery or Interpolation Error

Our error analysis in previous sections focussed on the conditioning and digital encoding of a continuous analog signal for subsequent manipulation within a computer. Yet, the design/analysis of computer real-time data conversion and recovery systems must be considered jointly. Signal recovery involves a digital-to-analog converter (DAC) followed by a bandlimiting function (e.g. linear first-order-hold (FOH), RC orButterworth filter, closed-loop control system, etc.) to attenuate the repetitive sampled-data frequency spectra down to its true baseband spectra (Figure 2.12 by Garrett). By itself, the DAC merely provides the ZOH step-interpolated representation of the signal with its associated amplitude and phase error (assuming zero computational delay). The output interpolator will provide signal filtering more ideal than the ZOH (see section 2.3 and the example error budget Figure 2.4). By including this improved interpolator, an error budget for the entire control structure will allow replacement of the large intersample error of signal conversion with the interpolation error of signal recovery.

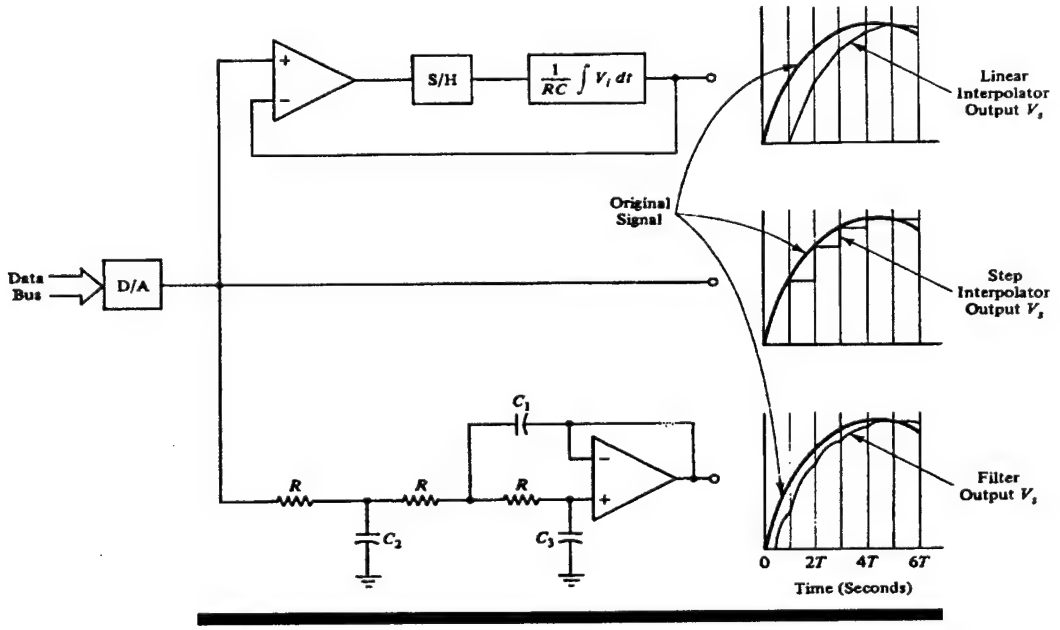


Figure 2.12 Signal Recovery Techniques

Garrett derives the interpolation error in the frequency domain from the achieved mean-squared-error (MSE) of the sampled-data signal. [Garrett] The MSE relationship has the dimension of rms volts squared and is depicted by signal image spectra existing above the baseband. For an input sinusoid, the MSE of the DAC output is the infinite sum of each spectral image's power as attenuated by the sinc amplitude response of the ZOH (Equation 2.16). This representation of the unwanted spectral images or noise can be approximated by considering only the first term with a constant 1.644 multiplier (Equation 2.17). [Brockman]

$$MSE = V_{rms}^2 \sum_{k=1}^{\infty} \left[\mathrm{sinc}^2\left(k - \frac{BW}{f_s}\right) + \mathrm{sinc}^2\left(k + \frac{BW}{f_s}\right) \right] (rms)^2 \qquad (2.16)$$

$$MSE = 1.644\ V_{rms}^2 \left[\mathrm{sinc}^2\left(1 - \frac{BW}{f_s}\right) + \mathrm{sinc}^2\left(1 + \frac{BW}{f_s}\right) \right] (rms)^2 \qquad (2.17)$$

The output SNR and interpolation error (Equations 2.18,2.19) for a coherent signal (as per section 2.2) are computed directly from the signal MSE.

$$SNR_{out} = \frac{V_{FS}^2/2}{MSE} \quad \frac{(rms)^2}{(rms)^2} \qquad (2.20)$$

$$\varepsilon_{interpolation} = \frac{100\%FS}{\sqrt{SNR_{out}}} \qquad (2.19)$$

$$\varepsilon_{interpolation} = \frac{\sqrt{2}\ \sqrt{MSE}}{V_{FS}}$$

$$= \sqrt{1.644}\ \frac{V_{pk}}{V_{FS}} \left[\mathrm{sinc}^2\left(1 - \frac{BW}{f_s}\right) + \mathrm{sinc}^2\left(1 + \frac{BW}{f_s}\right) \right]^{1/2}$$

This frequency-domain approximation for the DAC interpolation error can be proven equivalent to our time-domain approximation of intersample error (section 2.3.2) under proper operating conditions (large f_s/BW ratio).

When $\frac{f_s}{BW} > 10$ (proper operating conditions):

$$\varepsilon_{interpolation} = \sqrt{1.644}\,\frac{V_{pk}}{V_{FS}}\left[\left(\frac{BW}{f_s}\right)^2 + \left(-\frac{BW}{f_s}\right)^2\right]^{1/2}$$

$$= \frac{\sqrt{2}\,\pi\,BW\,V_{pk}}{\sqrt{6}\,f_s\,V_{FS}}\;100\%FS = \varepsilon_{intersample}$$

The interpolation/intersample error of the system is reduced upon considering the output filter's further attenuation of the signal's spectral images (Figure 2.13 by Garrett). A comparison of the performance of four output interpolators (Figure 2.14 by Garrett) highlights the convergence, with increasing order of interpolator, towards ideal signal recovery.

One concern in using an output interpolator is the associated time delay or phase lag of the signal-smoothing component. A basic tenet of control engineering is that this delay leads towards system instability. We can sidestep this problem by considering the intrinsic bandlimited response of the closed-loop system. For example, a first-order system response can be characterized by a single-pole RC filter which would perform as an improved interpolator during signal recovery. Interpolation error is determined with the RC filter equation of Figure 2.13.

Interpolator	$A(f)$	Output SNR	Delay
D/A	$\text{sinc}\,(f/f_s)$	$\dfrac{V_{FS}^2}{1.644\,V_S^2\left[\text{sinc}^2\left(1-\frac{BW}{f_s}\right)+\text{sinc}^2\left(1+\frac{BW}{f_s}\right)\right]}$	$\dfrac{1}{2f_s}$
Linear	$\text{sinc}^2\,(f/f_s)$	$\dfrac{V_{FS}^2}{V_S^2\left[\text{sinc}^4\left(1-\frac{BW}{f_s}\right)+\text{sinc}^4\left(1+\frac{BW}{f_s}\right)\right]}$	$\dfrac{1}{f_s}$
1-pole RC	$[1+(f/f_c)^2]^{-1/2}$	$\dfrac{V_{FS}^2}{V_S^2\left[\text{sinc}^2\left(1-\frac{BW}{f_s}\right)\cdot A^2(f_s-BW)+\text{sinc}^2\left(1+\frac{BW}{f_s}\right)\cdot A^2(f_s+BW)\right]}$	$\dfrac{2f_c+nf_s}{4f_sf_c}$
Butterworth n-pole lowpass	$[1+(f/f_c)^{2n}]^{-1/2}$	($f_s \pm BW$ substituted for f in $A(f)$)	

Figure 2.13 Output Interpolator Equations

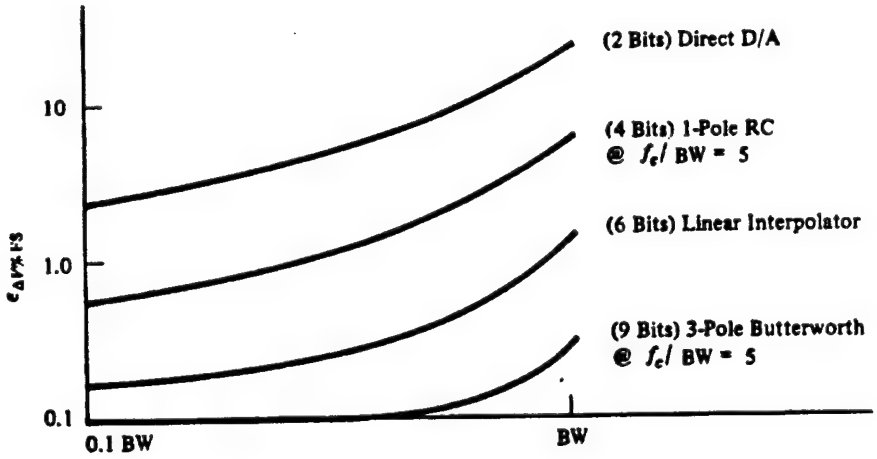


Figure 2.14 Output Interpolator Comparison

2.5. Conclusions

The analysis of a typical control structure provides a tabular form (or error budget) for itemizing, quantizing, and minimizing worst-case errors of an average, random, or systematic nature. The result is a stationary, Gaussian error function of minimal mean and variance conditioned on the reliable performance of the control structure. This probability density function defines the uncertainty of the control structure at any given point in time of its operation (i.e. what exactly is the value of the control signal u?). However, we are also uncertain as to whether the control structure is operating properly at this stage in its lifetime or mission. This uncertainty is represented by the probability density function of the control structure's reliability as a function of time. The following chapter reviews reliability theory and proposes a failure rate budget (the conceptual equivalent to the error budget) which will be the basis for the reliability pdf of the control structure.

Chapter 3: Analysis of Redundant Structures

Human capabilities to conceptualize many systems with accurate, real-time process models have been challenged. Instead of modelling the process, an error analysis of the control structure provides a minimized Gaussian error function (Chapter 2) by accounting for all sources of error in a tabular form. In a similar fashion, a reliability analysis of the control structure provides a maximized exponential reliability function (Section 3.3) by tabularizing all component failure rates. These models provide a complete concept of all a priori knowledge of the control structure. Entropy provides a measure of this a priori knowledge or, more appropriately, lack of knowledge (i.e. ignorance/uncertainty) in terms of the modelled probability functions (Chapter 5). It is found that these functions conform to Jaynes' method of maximum entropy where a chosen model remains minimally prejudiced with respect to any missing information. Thus, our error and reliability models exhibit a dualism in their origination and application. Further, these models can be optimized with respect to each application based on the give-and-take between the costs of various sources included in the error and failure rate budgets.

Redundancy allows further improvement of the control structure's error and reliability. For example, the deviation in the error function of the control signal is reduced through the averaging of the redundant outputs, owing to the essentially uncorrelated error contributions of each structure's elements (Section 3.2). This reduction in error variance is shown to be optimal with respect to redundant hardware for two structures. Analysis of redundant structures shows additional benefits in improved reliability (Section 3.4) occurring with each level of redundancy. Each additional structure in a redundant configuration provides an order of magnitude improvement in the reliability of the configuration during short term missions or earlier periods of extended operation.

However, these benefits are only possible at the cost of increased entropy or uncertainty with each level of redundancy (Chapter 5). An attempt to recoup these losses via fault detection and isolation (FDI) techniques is presented in Chapter 4.

The Dual-Difference Redundant Structure (DDRS) is based on two identical control structures (Figure 3.1). Redundancy may be in part (semi-redundancy, Figure 3.2) or in full (from sensors to actuators) for the control structure presented in Chapter 2 (Figure 2.2). As with a single control structure, the DDRS may be implemented directly within the inner loop for digital control (Figure 3.3) and/or removed to an outer loop to observe the process (Figure 3.4). Note that the process is <u>not</u> included within the DDRS. This becomes a key issue in Chapter 4 which highlights the direct, intuitive nature of our fault detection scheme and distinguishes it from other current research which emphasizes process modelling.

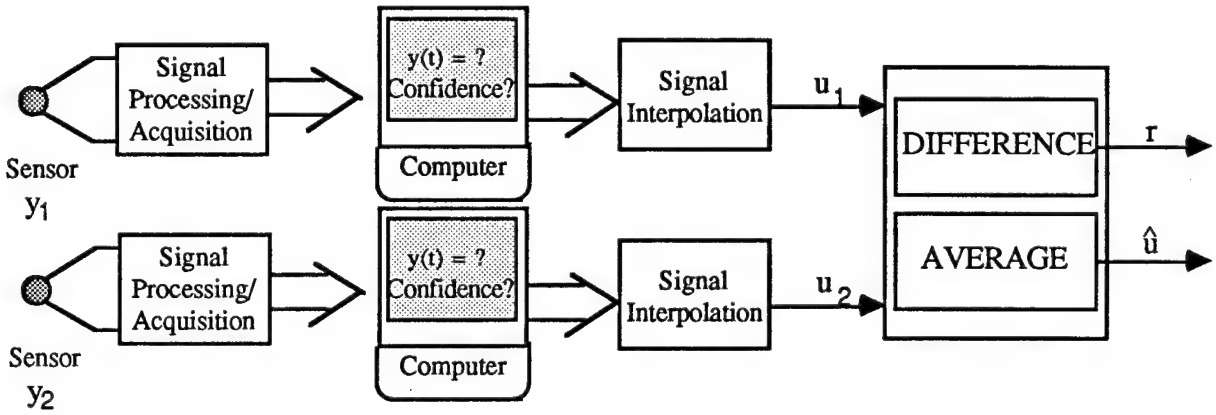


Figure 3.1 Dual-Difference Redundant Structure

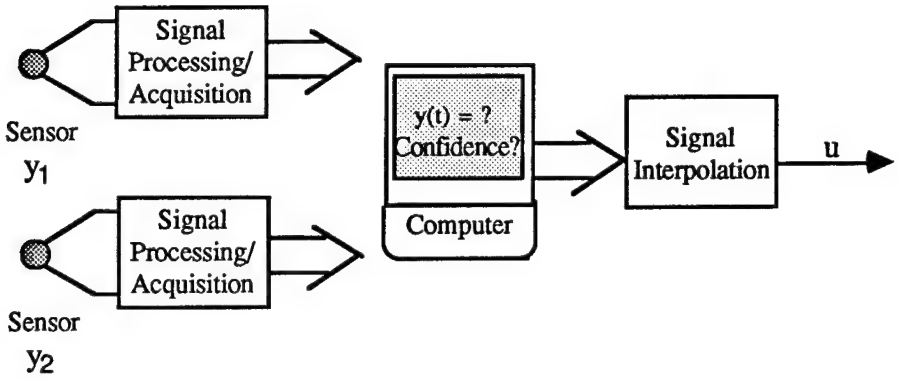


Figure 3.2 Dual Semi-Redundant Structure

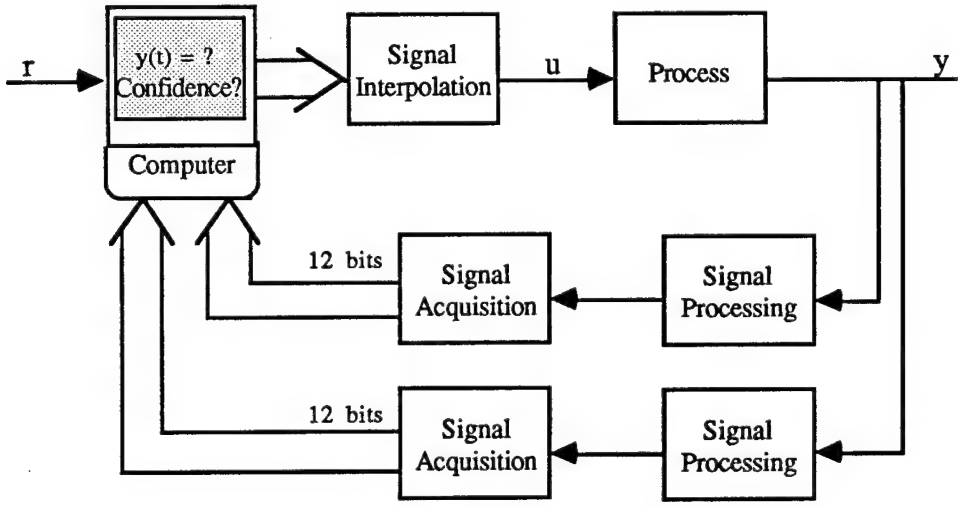


Figure 3.3 Inner Loop Digital Control

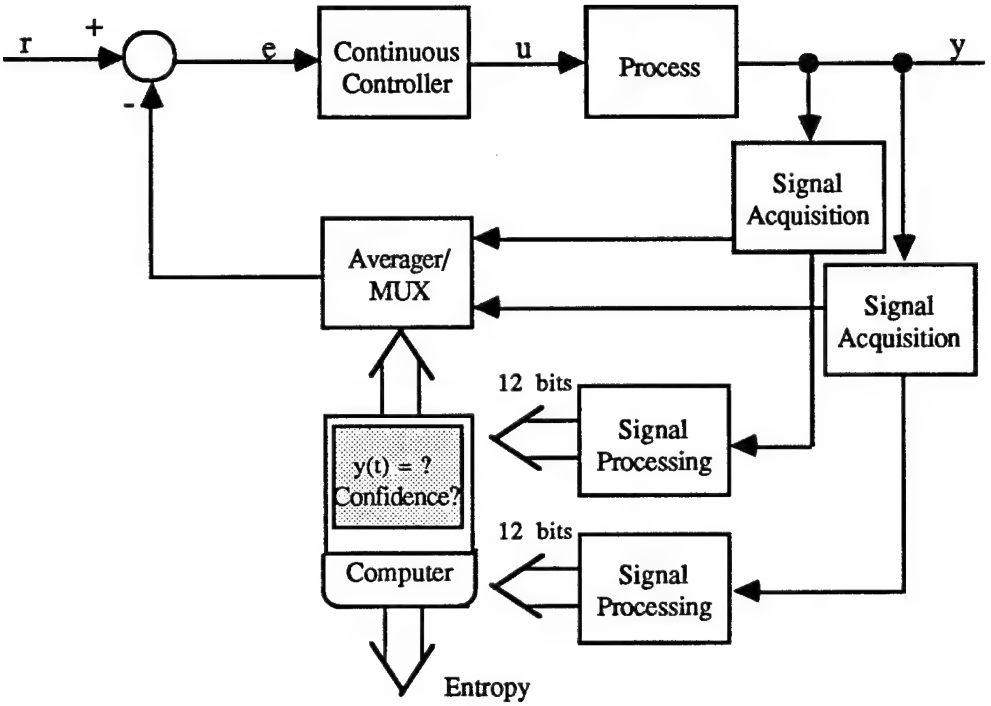


Figure 3.4 Outer Loop Observer/Planner

3.1. Redundancy

Traditional majority-voting schemes dictate the use of redundant control structures for fault-tolerant control. Redundancy is defined as the property of a device or system wherein it has more than one means of performing its function. This redundancy consists of spare modules, complete spare hardware structures, or analytical models which are available to mask faults (passive redundancy) or be switched on-line in the place of faulty modules or structures (active redundancy). For active redundancy, these spare systems may be 'hot' (i.e. continuously processing) and can therefore be switched in to control the process with little or no disruption. Status information may be shared between redundant structures to verify their performance and averaging will provide a best estimate of the control output. If a fault is detected, system reconfiguration entails either switching the faulty structure off-line or simply not including it within the averaged output; thereby, continuous system control is maintained but at reduced efficiency. Synchronization allows this sharing of data between redundant structures on a real-time basis and minimizes the interruption in active control of the process during switchover. In a loosely coupled system, the processors would run asynchronously due to their separate clocks; therefore each processor would have to stop at intermediate places called checkpoints so that they could check on the each other's performance. An alternate form of active redundancy allows the spare systems to be 'standby' (i.e. not processing) but this can cause a much larger switchover delay. Here, the spare system can monitor the process and take over when a lack of control is detected. System reconfiguration entails utilization of the spare modules or structures for piecewise replacement of faulty parts, thereby allowing continued system control at the same efficiency but only after a sometimes substantial delay. [Walker]

Triple modular redundancy (TMR) is the most common form of passive redundancy. Three hot, identical control structures are used to mask a fault on any single structure. A mid-value selection algorithm selects the middle value of the three output

control signals. This algorithm provides essentially perfect coverage for the first failure, since in order for a failed structure's signal to be selected for control of the process it would have to be in the middle of the two valid structure's signals. In addition, this algorithm allows continuous system control with zero recovery time for the first failure. Finally, this algorithm requires no intensive computations or processing because no fault detection is attempted and therefore no computer is required. It is this simplicity of the TMR concept that has made it one of the most popular designs for fault-tolerant control. The primary disadvantage of TMR is that it is unlikely for the mid-value selection algorithm to select the valid output signal in the event of a second failure (1 in 3 chance). The TMR concept can be expanded to N modular redundancy (NMR) so that (N-1)/2 failures can be tolerated. For example, the space shuttle's main computer uses a 4MR scheme. However, the use of passive redundancy to screen out the effects of the first failed structure is in many cases an insufficient response to the presence of a failure in a system. [Walker]

The DDRS is based on two identical control structures (Figure 3.1) whose sampling is synchronized by a common sync pulse from the computer. Both structures of the DDRS are hot and their outputs are averaged ($\hat{u}$) in order to ensure agreement in their control demands. The deviation σ_u in the conditional error function (Equation 3.1) is reduced through the averaging of redundant outputs, owing to the essentially uncorrelated error contributions of each structure's elements. The controller outputs are also differenced in order to check for consistency in their operation. This provides a sufficient statistic or residual (r) for fault detection (Equation 3.2). The common bias or mean value μ_r of the error function is removed (i.e. reduced to zero) upon differencing and the deviation σ_r is increased. Status information is shared at the computer and, if one structure is found faulty, then system reconfiguration consists of ignoring the failed controller's input in determining the output control signal. Of course, this causes a subsequent increase in the system error (using Equation 2.1) and unreliability.

$$\mathcal{E}(x \mid \text{Both Structures Reliable}) = \text{Gaussian}\left(\mu_u = \mu,\ \sigma_u = \sqrt{\frac{1}{2}\sum \varepsilon^2_{\text{random}} + \frac{1}{2}\sum \varepsilon^2_{\text{systematic}}} = \frac{\sigma}{\sqrt{2}}\right)$$

Conditional Error function of Average (Equation 3.1)

$$r(x \mid \text{Both Structures Reliable}) = \text{Gaussian}\left(\mu_r = 0,\ \sigma_r = \sqrt{2\sum \varepsilon^2_{\text{random}} + 2\sum \varepsilon^2_{\text{systematic}}} = \sigma\sqrt{2}\right)$$

Conditional Error function of Residual or Difference (Equation 3.2)

3.1.1. Error Analysis of Redundant Structures

The combined sensor-to-actuator error budget tabulated in Figure 2.4 defines the standard deviation σ of the conditioned error function for the control structure under normal operating conditions. This error variance can be further reduced through the averaging of multiple identical structures, as defined in equation 3.4, owing to the essentially uncorrelated error contributions of each structure's elements. [Raemer] Evaluation of this equation for N structures discloses a 30% reduction in combined error for two parallel controllers and a requirement for six controllers to duplicate this amount of improvement for 60% reduction in error. This result identifies an optimization of error reduction and redundant hardware for two structures averaged! Under normal conditions, Equation 2.1 is used to determine the standard deviation for a single structure's Gaussian error function and Equation 3.4 is subsequently used for redundant structures.

$$\text{Average}(\sigma) = \frac{\sigma_1 + \sigma_2 + \ldots + \sigma_N}{N} = \frac{1}{N}\sum_{i=1}^{N} \sigma_i$$

$$\sigma_{\text{parallel}} = \frac{1}{\sqrt{N}} * \text{Average}(\sigma) = N^{-3/2} * \sum_{i=1}^{N} \sigma_i \quad \text{for N parallel structures}$$

$$\sigma_{\text{redundant}} = N^{-3/2} * N * \sigma = \frac{\sigma}{\sqrt{N}} \quad \text{for N identical parallel structures}$$

(Equation 3.3, 3.4)

Under faulty conditions, the error deviation is drastically increased. A uniform fault distribution is assumed for the control structure where the fault magnitude is allowed to achieve any magnitude up to fullscale (FS) value for the control parameter with equal probability. A uniform probability density of base width $\alpha = 2FS$ has a standard deviation of 0.577 FS by Equation 3.5: [Peebles]

$$\sigma_F = \frac{\alpha}{\sqrt{12}} = \frac{2\ FS}{\sqrt{12}} \quad \text{for failed structure with uniform fault density}$$

(Equation 3.5)

This error variance can also be further reduced through the averaging of multiple identical structures, as defined in equation 3.3, owing to the essentially uncorrelated error contributions of each structure's elements.

$$\sigma_{NF} = \frac{\sigma_F}{\sqrt{N}} = \frac{2\ FS}{\sqrt{12N}} \quad \text{for N failed, identical, parallel structures}$$

(Equation 3.6)

Finally, redundant structures have possible system states which consist of n failed structures and m working structures ($n+m \leq N$). Equation 3.7 is utilized to determine the resultant error deviation for this system state of the redundant structure.

$$\sigma_{nF} = \frac{\sqrt{n}}{n+m}\,\sigma_F = \frac{\sqrt{n}}{n+m}\,\frac{2\ FS}{\sqrt{12}} \quad \text{for n failed and m working structures}$$

(Equation 3.7)

The Central Limit Theorem dictates that the probability density function of the sum of a large number of random variables approaches a Gaussian distribution. In particular, Peebles found that the summation of independent uniformly distributed random variables can be closely approximated by a Gaussian density with equivalent mean and variance; even for the case of only two variables summed. Hence, the conditional error distribution for a redundant control structure with two or more failures ($n \geq 2$) is represented by a Gaussian density with zero mean and standard deviation of σ_{nF}. Otherwise, the conditional error distribution for a redundant structure with one failure ($n = 1$) is uniform with a base width of $\alpha_N = \alpha/N = 2FS/N$.

3.2. Reliability

Reliability (R) is frequently considered to be the capacity of a module or system to preserve its operating characteristics within given limits and under specific conditions of stress to achieve the mission of interest. It represents the a priori cumulative distribution for the probability f(t) of system failure time t_f (i.e. when the system passes beyond its given limits) from the given time t to infinity. The most useful way to express the (un)reliability and its associated pdf is in terms of the system failure rate (λ) or its inverse, mean time between failures (MTBF). The MTBF is the expected time during which the system will perform properly between or until failures. Component failure rate (λ_i) can be estimated from observations over numerous testing cycles and is usually provided by the manufacturer in terms of MTBF (Equations 3.8, 3.9).

$$\text{Component Failure Rate } (\lambda_i) = \frac{1}{\text{MTBF}}$$

$$\text{Estimated Component Failure Rate } (\hat{\lambda}_i) = \frac{\text{\# failures observed}}{\text{\# units tested} \times \text{ hours tested}} \cong \lambda_i$$

(Equations 3.8, 3.9)

The probability of system failure for a given time (density function f(t), Equation 3.10) or over a given time period (Unreliability distribution Q(t), Equation 3.12) can then be evaluated. [Walker]

The behavior of λ over time is typically represented by the "bathtub" curve (Figure 3.5). During the early failure period, weak parts that are marginally functional are eliminated within the first few hours of operational burn-in. The middle section of the curve, or the useful life period, contains the smallest and most nearly constant failure rate. Here, the reliability of a component or system which is subject to failure due to a large number of independent causes is characterized by an exponential pdf (Figure 3.6, Equation 3.11) much in the same way that the normal is a limiting distribution for the error (as

dictated by the Central Limit Theorem, Chapter 1) [Drenick]. This dualism is further exhibited in that both the error and reliability distributions are maximized with respect to entropy (see Section 3.5.1). In the final section of the bathtub curve, device strength deterioration causes wearout failures to overcome these chance failures during the last span of system life. Thus, the complete history of system reliability is defined by the history of the failure rate. The useful life span of the system is the focus of our discussion. [Bazovsky]

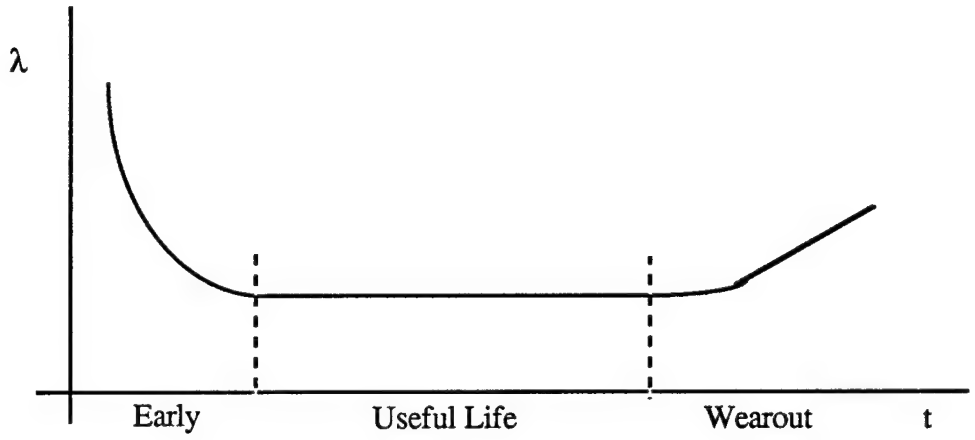


Figure 3.5 Failure Rate Bathtub Curve

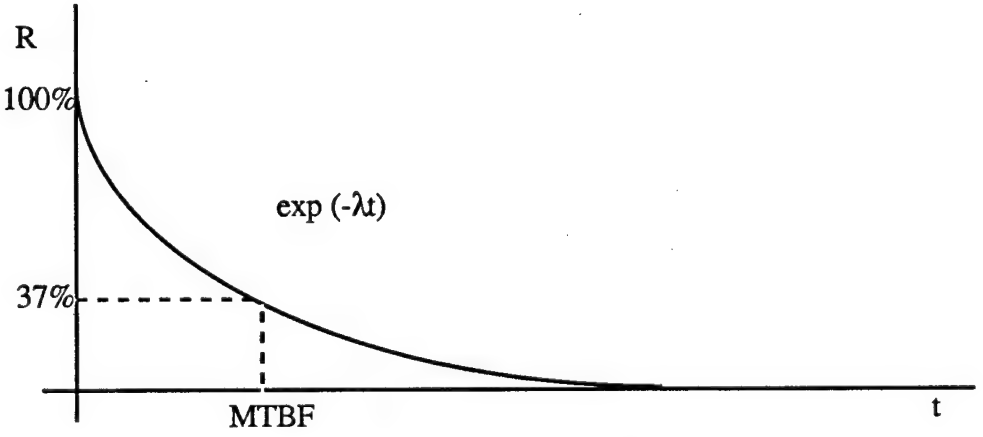


Figure 3.6 Reliability Exponential PDF during Useful Life

Component Failure pdf $f_i(t) = p(t = t_f) = \lambda_i \exp(-\lambda_i t)$ (Equation 3.10)

Component Reliability $R_i(t) = p(t < t_f) = \int_t^{\infty} f_i(\tau)\, \partial\tau = \exp(-\lambda_i t)$ (Equation 3.11)

Component Unreliability $Q_i(t) = p(t \geq t_f) = \int_0^{t} f_i(\tau)\, \partial\tau = 1 - \exp(-\lambda_i t)$ (Equation 3.12)

The characteristic property of the exponential distribution which is associated with the useful life period of a system is its constant failure rate or lack of memory property. A component does not "remember" how long it has been in operation (i.e. how many times it has been used). Thus, the probability it will fail in the next hour of operation (Equation 3.12) is the same if it were new (i.e. unused), regardless of its accumulated power-on hours. Failure becomes merely a chance occurrence. An additional characteristic of the exponential distribution is the closure property of failure rates for serial systems. The failure rate of a serial system, where M components operate independently and the system fails when the first component fails, is the sum of all M component failure rates (λ_i). The control structure can be considered a serial system of independent components (Figure 2.1), each with their own respective component failure rates. An example tabulation of component failure rates and their summation for structure failure rate (λ_{total}) is presented in Figure 3.7. By the independence assumption, the reliability probability of a serial system is the intersection or product of all component reliabilities (i.e. all components must be working for the system to work) (Equation 3.13). Thus, the exponential distribution allows the closure property on failure rates for serial systems. Structure unreliability for each controller in the DDRS is the complement of the structure reliability (Equation 3.14). [Bazovsky]

Structure Reliability $R_S = R_1 \cap R_2 \cap \cdots R_M$

$$= \exp(-\lambda_1 t) * \exp(-\lambda_2 t) * \cdots \exp(-\lambda_M t)$$

$$= \exp(-(\lambda_1 + \lambda_2 + \cdots \lambda_M) * t)$$

where M = number of components within the structure

$$\text{Structure Reliability } R_S(t) = \prod_{i=1}^{M} R_i(t) = \prod_{i=1}^{M} e^{-\lambda_i t} = e^{-\lambda_S t} \text{ where } \lambda_S = \sum_{i=1}^{M} \lambda_i$$

(Equation 3.13)

$$\text{Structure Unreliability } Q_S(t) = 1 - R_S(t) = 1 - e^{-\lambda_S t}$$

(Equation 3.14)

Component	Failure Rate (per hour)	Comments
Sensor	10^{-6}	Thermocouple
Interface	10^{-6}	Cold-junction Compensation
Filter	10^{-5}	1-pole RC
Amplifier	10^{-5}	OP-07
Multiplexer	10^{-5}	CMOS
A/D Convertor	10^{-4}	12-bit conversion
Computer	10^{-5}	IBM AT
Structure Failure Rate (λ_S)	0.000142	Summation of component rates
Structure MTBF	7042 hours	Inverse of failure rate

Figure 3.7 An Example Structure Failure Rate Budget

The need for higher levels of reliability increases with the economic, hazardous, or other consequences of equipment failure and downtime. Common methods of reliability enhancement or fault avoidance include: operating at low stress (derating), design simplification to increase component reliability, specification of premium components (as opposed to industrial grade parts passed within $\pm 3\sigma$ of spec), and redundancy. In applications where low front end failure rates have higher priority over component cost (e.g. the computer systems on the space shuttle), redundancy of key parts of the system is a commonly used option. The parallel redundancy of the DDRS allows system reliability greater than that of a single control structure. Due to the independent operation of the parallel structures, the system unreliability of a parallel system (Equation 3.15) is the intersection or product of all structure unreliabilities (all structures must fail for the system to fail). Since each probability is between zero and one, system unreliability will be less than either structure's unreliability. As with the serial and parallel error equations, semi-redundant structures must make use of both equations 3.14 and 3.15 in determining system unreliability.

Parallel Redundant Structure Unreliability $Q_P(t) = \prod_{i=1}^{N} Q_S(t) = (1 - e^{-\lambda_s t})^N$

(Equation 3.15)

Parallel Redundant Structure Reliability $R_P(t) = 1 - Q_P(t) = 1 - (1 - e^{-\lambda_s t})^N$

(Equation 3.16)

3.2.1. Reliability Analysis of Redundant Structures

The relative improvement in reliability which can be achieved by employing active redundancy is illustrated in Figure 3.8 by Walker. In this figure, the unreliability of a single structure is compared to the unreliabilities of a dual and triple redundant configuration of identical control structures. The unreliability q of each configuration is plotted as a function of a ratio of the period of operation t and the structure's mean time between failures τ $(1/\lambda_S)$. It can be seen that the maximum benefit of redundancy is achieved during early operating periods with respect to the structure's MTBF. In the limit as the ratio t/τ goes to zero, the slopes of the curves approach N decades per decade (where N = number of structures in the configuration). Thus, each structure in a redundant configuration provides an order of magnitude improvement in the reliability of the configuration during short term missions or earlier periods of extended operation. However, as the ratio t/τ approaches unity, the reliabilities of all configurations approach zero and the benefits of redundant structures, although present, become less dramatic. This reflects the fact that the probability that even one of the identical structures will still be operating at MTBF τ is small no matter what level of redundancy was employed. From this analysis, one can see the tremendous benefits in reliability possible with large configurations of active structures or with hybrid redundancy (any combination of active and standby redundancy). A hybrid redundancy scheme, consisting of a number of active control structures (e.g. DDRS) employed for efficient fault tolerance and a number of standby control structures which can be switched into the active configuration upon the occurrence of a fault or before the MTBF is reached, can achieve any specified reliability goal with less reliable components than simply an active redundant scheme. Of course, the additional hardware requires more expense and working volume than can usually be afforded. In fact, space limitations and expense are two major reasons why redundant structure configurations are avoided and research has shifted to analytical redundancy. [Walker]

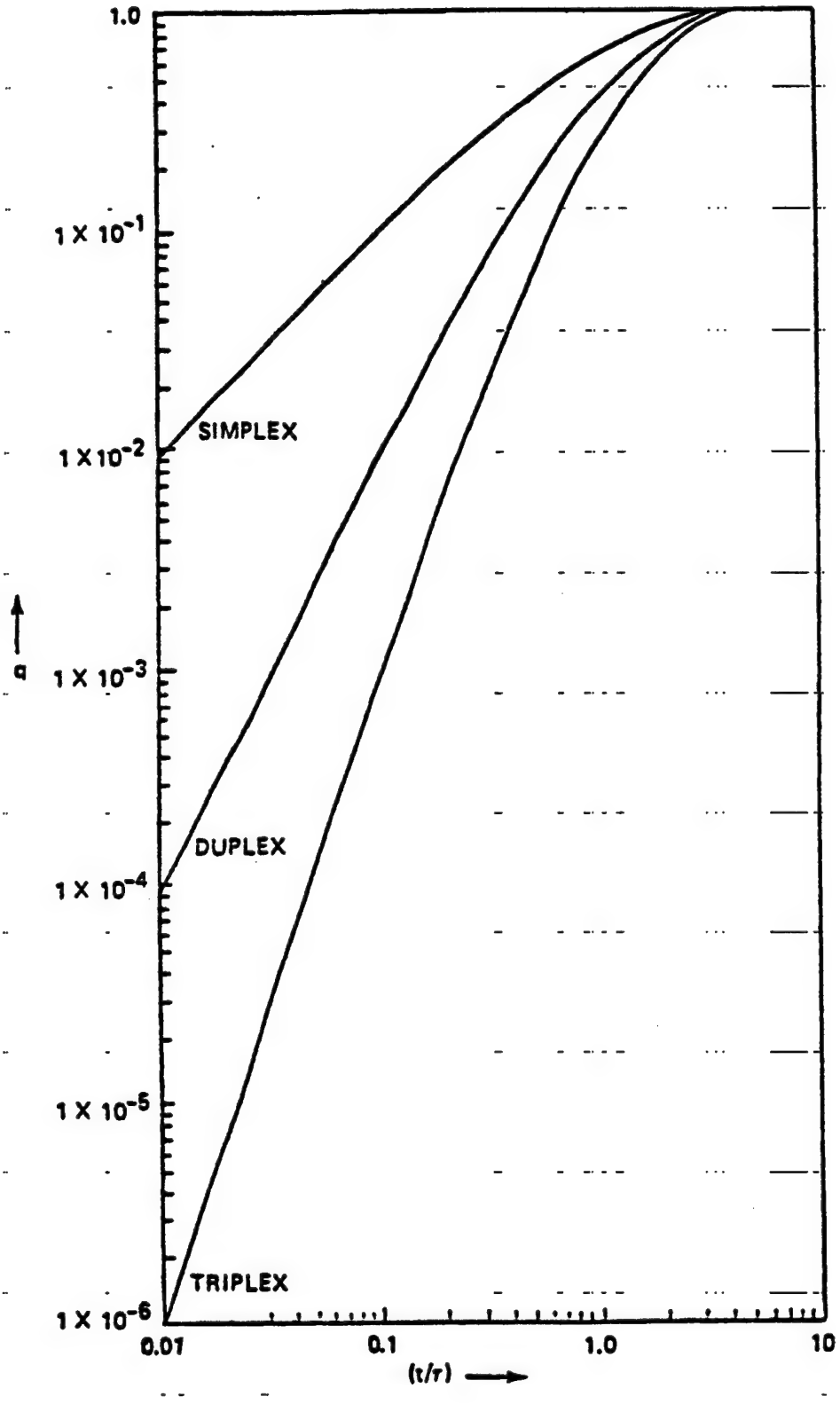


Figure 3.8 Unreliability Comparison of Redundant Configurations

3.2.2. Effect of System Inspection on Reliability

As discussed above, system reliability is represented by an exponential function during its useful life period (Figure 3.6) with an estimated mean time before failure (MTBF = $1/\lambda$). The exponential distribution is characterized by a lack of memory property; its form is consistent over numerous missions during its useful life span, irregardless of the number or length of the missions. However, this property assumes that the system is inspected for faults between missions and found to be operational. The following analysis proves the lack of memory property of the exponential distribution for failure time (Equation 3.10). Here, the system is inspected at time t_I and found to be operating normally. Thus, the time of failure t_f for the system must be greater than the time of inspection ($t_f > t_I$). The conditional probability of system failure time given normal operation at the time of inspection is determined in Equation 3.17. [Peebles] The result is that the inspection time becomes the new start time or zero reference for the exponential distribution associated with reliability and failure time. The distribution maintains its form and is simply shifted in time to the right.

$$\text{Failure time } f(t \mid t > t_I) = \frac{\partial}{\partial t} \frac{Q(t) - Q(t_I)}{1 - Q(t_I)} = \lambda \exp(-\lambda [t - t_I]) \text{ for } t \geq t_I \qquad \text{(Equation 3.17)}$$

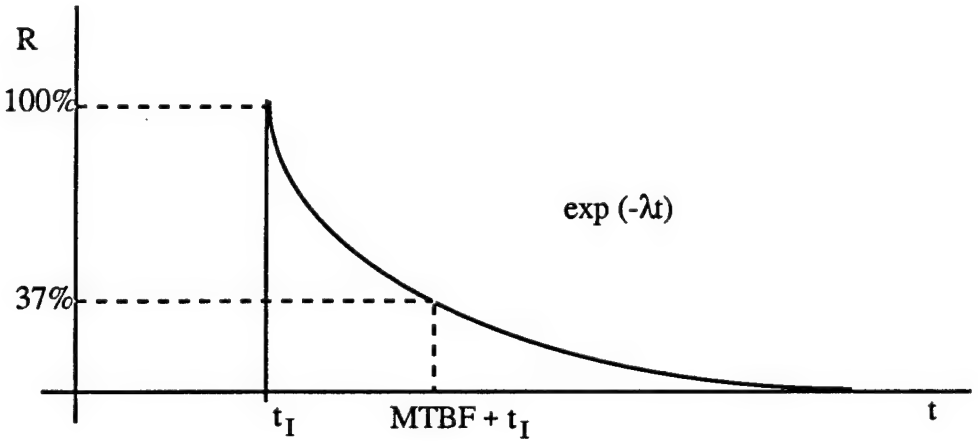


Figure 3.9 Reliability Exponential PDF after System Inspection

3.3. Conclusions

The control structures presented in this thesis are designed for the benefits of redundancy. The deviation in the error distribution of the control signal is reduced through the averaging of the redundant outputs, owing to the essentially uncorrelated error contributions of each structure's elements. This reduction in error variance is optimal with respect to redundant hardware for two structures. The controller outputs are also combined in order to provide a sufficient statistic or residual for fault detection and isolation (FDI). Each structure in a redundant configuration provides an order of magnitude improvement in the reliability of the configuration during short term missions or earlier periods of extended operation. However, redundancy also causes an increase in system entropy with respect to reliability and accuracy.

The results of previous sections on reliability have assumed perfect coverage of all possible faults or deviations from normal operation for the control system. Coverage is the property of a system which defines its ability to tolerate failures of a specified subset or percentage of its components (i.e. the degree of its fault tolerance). The mid-value selection algorithm of the TMR concept allows coverage of only the first failure and the NMR concept allows coverage of the first (N-1)/2 failures where N is any integer. However, the improvement in structure reliability with each level of redundancy assumes that: 1) a fault to any single controller has no effect on the normal operation of the total control system, and 2) the total control system fails only upon the failure of all controllers. This is only possible with perfect fault detection and isolation (FDI) and subsequent reconfiguration of the control system to maintain normal operations without loss in performance (i.e. complete fault coverage). In the following chapters, we shall investigate the fault coverage and reduced system entropy achieved by FDI schemes for dual and triple redundant control structures.

Chapter 4: Fault Detection and Isolation (FDI)

In contrast with current fault-tolerant control schemes, the dual-difference redundant structure (DDRS) and triple redundant structure (TRS) provide real-time failure detection and error accountability for sensor systems in an untended manufacturing environment without the use of a process model. Instead of modelling the process, an analysis of the control structure provides a minimized Gaussian error distribution (Chapter 2) and a maximized exponential reliability distribution (Chapter 3). These models provide a complete concept of all a priori knowledge of the control structure. Entropy provides a measure of this a priori knowledge or, more appropriately, lack of knowledge (i.e. ignorance/uncertainty) in terms of the a priori probability distributions (Chapter 5).

Thus, the DDRS and TRS are one step beyond passive redundancy schemes (e.g. TMR or NMR) towards complete fault coverage in that fault occurrences are detected and not merely screened. Also, these control structures provide fault-tolerant control (i.e. fault detection, isolation, and reconfiguration) to the extent of their capabilities. The dual-difference redundant structure provides quick and efficient front-end fault detection with a simple difference test, yet fault isolation is only possible to the extent which the simplex fault detection schemes provide fault coverage. The triple redundant structure, however, provides both efficient fault detection and isolation with a more complex FDI scheme. Upon fault detection, the TRS is reconfigured to the DDRS with the two remaining valid controllers. In this manner, fault-tolerant control is achieved.

Many current FDI techniques rely on a systems approach to dictate the proper operating conditions for a controller. The emphasis of a systems approach is upon understanding the process (not the control structure) so that its progress can be controlled and faults contained. There are several problems with this approach:

1. Fault detection for the control structure is achieved in a secondary fashion. Generally, these efforts involve using a process model (numeric or symbolic) to estimate the process outputs (y) for given inputs (u), and these are compared with the input sensor readings of the controller. Any major discrepancy indicates the occurrence of a fault. Attention must be focussed upon the control structure, not swept along with process modelling, for its proper fault monitoring.

2. These models usually cannot represent the process completely and there is some considerable error associated with their estimates. It is the assumption of this paper that our expert model of the control structure allows greater confidence than any results achieved with a process model due to a smaller variance.

3. There is no generic model which represents every process effectively. It is the goal of this paper to model a generic control structure (in broad terms, admittedly) such that it may be applied to any controller equally and effectively.

4. The ancient argument of empirical vs. theoretical belief. In this instance, it seems intuitively better to know with certainty what the process is doing rather than what it should be doing.

This is not to imply that the extensive work being done with analytical redundancy is not meaningful. On the contrary, we shall find that more efficient fault detection and isolation is possible with additional sources of information or voters. Of course, with this additional knowledge comes greater complexity. With analytical redundancy, confidence may shift to the system level in order to diagnose each controller's performance. Hence, local observation and process modelling can complement each other in order to ensure continuous and efficient system knowledge. Alternatively, an analytical model of the process can be used as a failsafe in the case of complete hardware failure. In this chapter, we shall confine our attention to the analysis of FDI schemes based upon physical hardware redundancy.

4.1. Off-line Maintenance

Important to the reliable performance of systems over long periods of operation is the use of scheduled maintenance. By use of partial disassembly, visual inspection, and a number of specialized inspection/testing procedures and equipments, deterioration of components can be discovered and the components replaced before they fail to perform in an adequate manner. Some stress testing may be included in maintenance procedures to identify components which are weak in some respect and are more likely to suffer an early failure. It is clear that frequent and careful scheduled maintenance is highly beneficial and yet is also costly both in terms of the personnel and facilities required to perform the maintenance and in terms of the additional systems required to continue service while others are out for maintenance. In addition, periodic testing cannot detect any transient faults or spurious noise sources unless they occur during the test. Therefore, some form of on-line or insitu FDI schemes are required. It is assumed that inspection of the redundant controllers is performed prior to any mission (see Section 3.2.2).

4.2. Simplex Fault Detection and Isolation

Self-tests of single or simplex structures can be implemented by adding additional hardware to the control structure or by incorporating reasonability tests in the computer software which monitors the structure's status. These self-tests are usually designed to detect those failure modes or their respective signatures which have been identified by conducting a failure modes and effects analysis of the control structure design. Although a self-test may quickly and efficiently detect the failure mode for which it has been designed, the inability to predict a priori all of the failure modes of the control structure tends to limit the coverage which the self-test provides.

Built-in Test Equipment (BITE) refers to special monitoring hardware or other means of directly indicating the operating condition of the control structure or one of its components or subsystems. For example, Analog Devices 4B Alarm Limit Subsystem is an off-the-shelf BITE which provides adjustable alarm limit modules with independent HI and LO relay outputs in order to monitor up to twelve control signals. A watchdog monitor (WDM) can be implemented in hardware or software which requires a specific action or sequence of actions to occur continually within a specified time period. Some sensor inputs that have two-winding inputs (e.g. resolvers, LVDTs, RVDTs) have known arithmetic relationships between the two inputs and can therefore be checked in this manner. Output integrity can be accomplished by wrapping the output signals, often in the form of a current, back to the control system for verification. However, the very nature of continuous test equipment contradicts itself in that the BITE itself is subject to faults as well.

Reasonability tests are the first line of testing done by the control structure to ensure the validity of the control structure. Limit testing of the controller variable and its rate will detect for extreme bias and noise conditions, respectfully, which comprise the majority of spontaneous faults. For example, if power to the signal acquisition and conditioning subsystems goes down or the signal line is cut or opened, then the input computer readings will take a giant step to some incoherent value (typically zero). In addition, the physical characteristics of the hardware (e.g. thermocouple) or the parameter may dictate an absolute minimum and/or maximum for the control signal. Thus, the range check may also guard against shorts to other voltage sources or across the control structures if the sudden bias is large enough to exceed the range. The rate check compares the discrete rate of change from sample to sample versus the maximum for that parameter. Thus, the rate check may be able to detect a short to a noisy source or the occurrence of a transient spike disturbance.

Additional reasonability tests can be constructed to account for other directly observable fault characteristics of the simplex control structure.

The implementation of a self-test introduces the risk of making two types of decision errors in assessing the performance of the control structures (Figure 4.1). One might erroneously decide that an unfailed structure has failed and this decision error is referred to as a false alarm (FA) or a Type I error. Alternatively, one might erroneously decide that a failed structure has not failed and this decision error is referred to as a missed detection (MD) or a Type II error. Either decision error can arise from failures of the BITE hardware. Missed detection is a common decision error for reasonability tests when the magnitude of the fault is not large enough to exceed the specified intervals. These decision errors can have a significant impact on the reliability and performance of the control structure.

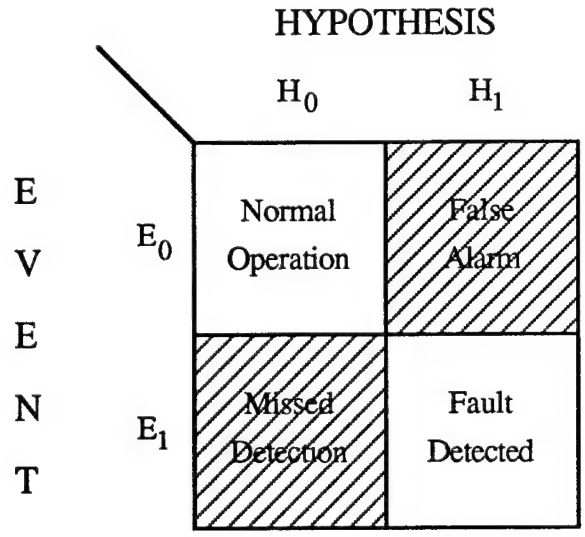


Figure 4.1 Two Possible Types of Decision Errors for a Binary Event Set

4.3. Duplex Fault Detection and Isolation

The dual-difference redundant structure (DDRS) is the logical implementation of our efforts to model the controller error sources (Chapter 2). By placing identical control structures side-by-side, we can validate their dual performance by comparison of the two structures. For a given common input at the sensors, what is the deviation between the identical structures? Notice that no knowledge of the input is needed, save that it is the same for both structures. The difference test will usually provide better coverage for structure faults than is provided by simplex testing because its effectiveness is not limited by an inability to predict a priori all of the possible failure modes. Its effectiveness is strictly limited by the uncertainties in the measurements (i.e. the error) and in the control structures (i.e. reliability). Ideally, controller deviation would be zero for all time. From our expert model of structure error, we know that this is not the case.

Structure error is represented by a stationary Gaussian pdf with minimal mean and variance (Equation 2.1). A 2-dimensional error vector $\bar{\varepsilon}$ (Figure 4.2) can be defined which takes a random walk within the space defined by the error of controller 1 (ε_1) and the error of controller 2 (ε_2). This space can be delimited by a box or window of width T. This threshold T can be optimally determined from a cost analysis of all possible event and hypothesis pairings for the dual structure (Bayes Criterion, Section 4.3.2). Alternatively, this "Window of Valid Performance" can be defined such that it confines the dual structure error vector for most samples during normal operating conditions (Neyman-Pearson Criterion, Section 4.3.3). For example, a threshold set at the three sigma limit confines a Gaussian variable for 99.7% of all samples under normal conditions. In either case, traversal of the error vector beyond this boundary implies the occurrence of a single or dual structure fault (where f_1, f_2 = magnitude of a fault in structure 1 and 2, respectively). A single structure fault involves the addition of a 1-dimensional error vector (horizontal or vertical), while a dual fault is 2-dimensional.

One problem, however, with any given setting of the window's size is that there is always the probability that this traversal is merely a valid magnitude of the modelled error vector. The probability of false alarm (P_{FA}) is this conditional probability of improper fault detection given that no such fault has occurred. The Neyman-Pearson criterion for determining the threshold T is based on maintaining a specific bound on P_{FA}. This draws our attention to the second problem in determining the decision threshold; the possibility of a missed detection (P_{MD}), where the window may be set too big relative to the fault vector's magnitude. Thus, there exists an inherent give-and-take for this scenario between false alarms and missed detections.

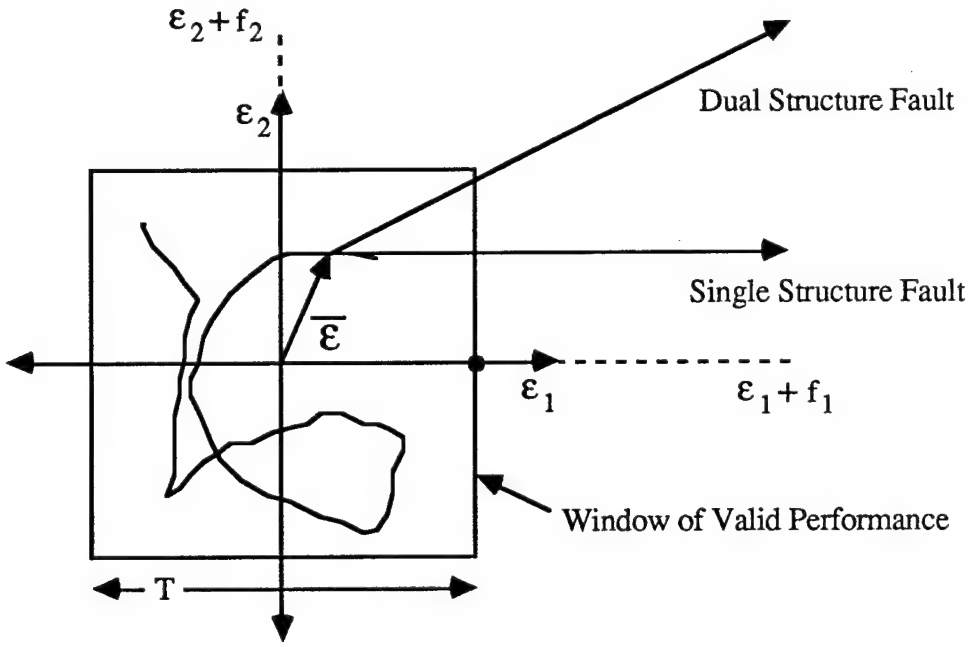


Figure 4.2 Dual Structure Error Space

The key to the DDRS is the parallel, redundant nature of the control path which allows increased confidence in the dual controllers due to their continual status cross-checking. Thus, any error sources common to both parallel paths in the DDRS such as process disturbances, load changes, improper sensor or actuator location, nonredundant modules in the control path, etc. cannot be considered in our DDRS fault analysis. Deviations of the measured parameter from expected values due to these error sources will be transparent to the difference test and must be detected with process knowledge by the host computer (the next level of diagnostics). Full redundancy, therefore, is preferred over partial or modular redundancy. Parallel operation is not always feasible, though, for all modules in the control path, such as: averaging two actuators to drive the process, space limitations in locating the two sensors, the expense of two redundant computers, etc.

4.3.1. Dual-Difference Validation Test

The combination of dual redundant control structures and an expert model of the structure error allows for a quick, efficient method of validating dual controller performance. Limit testing of the controller variables and their rates will detect for extreme bias and noise conditions, respectfully, which normally comprise the most costly of spontaneous dual and single channel faults. This definition of full scale magnitude (FS) corresponds to an additional, outermost square (Figure 4.3) in the dual structure error space which confines the error vector for all time. In addition to limit testing, a direct comparison (or difference test) of two controller variables (e.g. outputs u_1 and u_2) can validate DDRS operation with respect to the a priori error $p(\varepsilon)$ and reliability $R_S(t)$ distributions for the structures and a worst-case fault magnitude f_{min} based on the current application. This comparison can be performed at any point in the parallel path of identical structures, but can only validate the DDRS up to and not beyond that point. The residual r

is considered a sufficient statistic for this comparison because it removes the controller variable (u) and error mean (μ_ε), which are common to both signals, from the test. The dual-difference validation test is represented in Figure 4.3 by the area confined between two parallel lines (given in slope-intercept form: $\varepsilon_2 = \varepsilon_1 + T$ and $\varepsilon_2 = \varepsilon_1 - T$):

Difference Test for Validation of the Dual-Difference Control Structure
under normal operating conditions (i.e. $f_1 = f_2 = 0$)

$$| u_1 - u_2 | = | u + \varepsilon_1 + f_1 - u - \varepsilon_2 - f_2 | = | \varepsilon_1 - \varepsilon_2 | \leq T$$

$$\text{Hence,} \quad \varepsilon_1 + T \geq \varepsilon_2 \geq \varepsilon_1 - T$$

The Window of Valid Performance, however, is still a subspace of the space confined by the difference test. Figure 4.4 depicts the convergence of different validation schemes and their associated test spaces towards the desired limits set by our expert model. The Dual-Difference test space is shown to be smaller than that achieved through traditional majority-voting schemes because minimal error variance is assumed for the expert model.

The drawback of the difference test is that our detection scheme is also insensitive to a common bias fault: a dual fault where a fault of equal amplitude occurs on both controllers. The difference test attempts to define acceptable behavior of the error vector in the dual structure error space with the one-dimensional pdf of the residual r (Equation 3.2). The long strip cutting diagonally across the length of the error space represents the possible missed detection of a common bias fault. If a uniform, equivalent fault distribution is assumed for both controllers (the faults have an equal chance of achieving any magnitude up to full scale and, therefore, a fault vector has an equal chance of reaching any point in the error space), then the probability of the occurrence of a common bias fault can be based on the ratio of the area of this strip (A_{DT}) to the area confined by limit testing ($4\ FS^2$). For small threshold T, this ratio is approximated by T/FS.

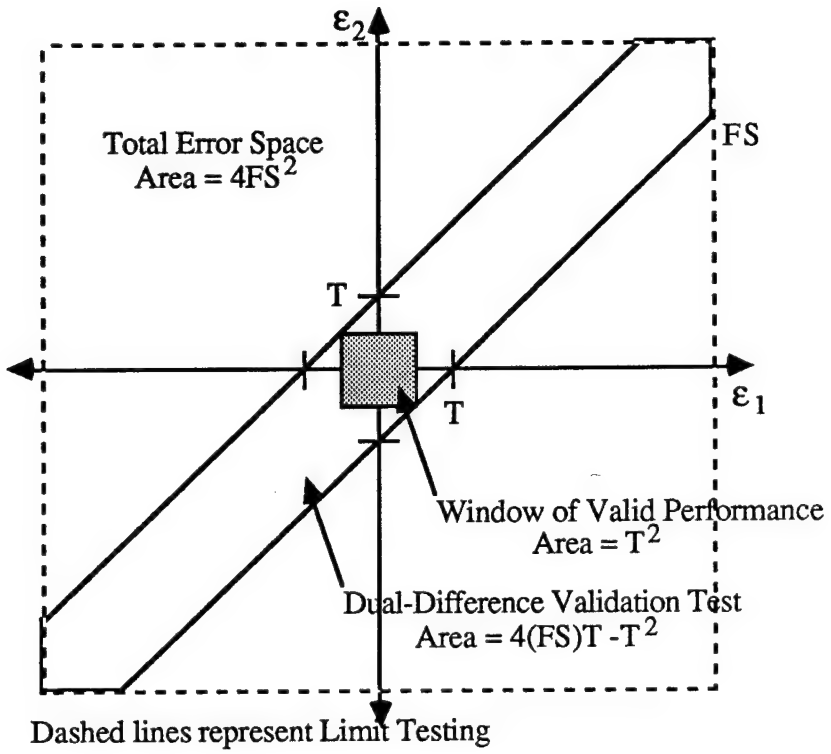


Figure 4.3 Dual-Difference Validation Space

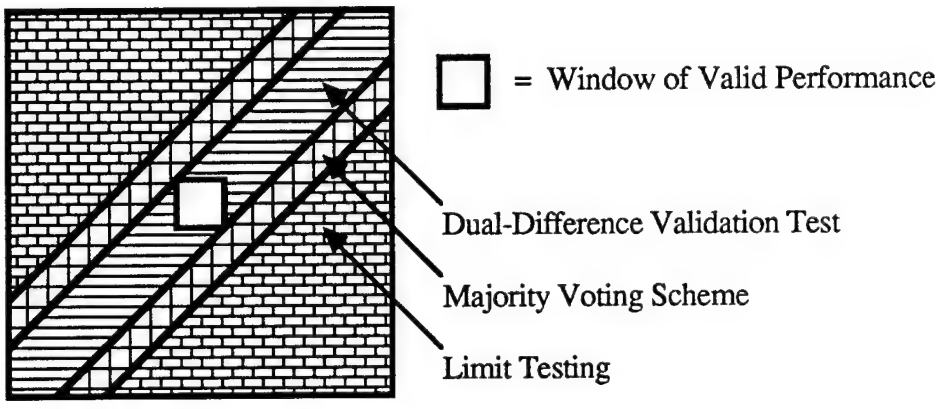


Figure 4.4 Convergence of Validation Schemes

4.3.2. Detection Scheme Optimization with Bayes Criterion

Our fault detection scheme is analyzed as a classical, M-ary hypothesis test (M=3) with a fixed, singular data sample. [Van Trees] With each sample, it is assumed that a decision from M possible decisions must be made as to which event of M possible events has occurred. Thus, there are M possible alternatives or event-hypothesis pairings each time a decision must be made. The three events E_0, E_1, and E_2 in our fault detection scheme are that no fault, a single fault, or a common bias fault has occurred, respectively. Our decision will be facilitated by a unique physical manifestation associated with each event (i.e. the magnitude with which each event affects the measurable residual r). Dual faults other than common bias faults are assumed to be indistinguishable from single structure faults with respect to the difference test and are, therefore, included in event E_1. This fact has important ramifications in our attempt to isolate a fault to the structure in which the fault occurred. Event E_1 is represented as an additive error of magnitude $f = f_1 - f_2$ (Figure 4.2) which causes a bias shift in the pdf of the residual r. This analysis is concerned with the worst-case magnitude of f (f_{min}) which is the smallest fault (and, thus, the hardest to detect) of accountable cost for the current application. A major concern is that event E_2 (a common bias fault) has no effect on the residual r and cannot be distinguished from normal operating conditions.

$$P_0 = p(E_0) = R_S^2(t); \quad P_2 = Q_S^2(t)\frac{A_{DT}}{FS^2} = Q_S^2(t)\left(\frac{4\,T\,FS - T^2}{4\,FS^2}\right); \quad P_1 = 1 - P_0 - P_2$$

Equations 4.1 - 4.3

$$p(r|E_0) = p(r|E_2) = p(r) = \frac{1}{\sigma_r\sqrt{2\pi}}\exp\left(-\frac{r^2}{2\sigma_r^2}\right)$$

Equation 4.4

$$p(r|E_1) = p(r - f_{min}) = \frac{1}{\sigma_r\sqrt{2\pi}}\exp\left(-\frac{(r - f_{min})^2}{2\sigma_r^2}\right)$$

Equation 4.5

Our fault detection scheme is optimized by using a generalized likelihood ratio test (GLRT) which is based on a degenerated Bayes criterion. [Van Trees] The Bayes criterion assumes the a priori determination of the event probabilities P_0, P_1, and P_2 (presented above); the conditional probabilities P_{00}, P_{01}, P_{02}, P_{10}, P_{11}, and P_{12} for each decision given the occurrence of each event (presented below); and the costs C_{00}, C_{01}, C_{02}, C_{10}, C_{11}, and C_{12} associated with each possible event-hypothesis pairing. For this exercise, the Bayes criterion is degenerated such that only two hypotheses are of importance (H_0 = valid performance, H_1 = fault detected) and only six alternate pairings are possible.

$$P_{00} = p(H_0|E_0) = P_{02} = p(H_0|E_2) = \int_{-T}^{T} p(r)\,dr = \mathrm{erf}\left(\frac{T}{\sigma_r\sqrt{2}}\right) = \mathrm{erf}\left(\frac{T}{2\sigma}\right)$$

$$P_{FA} = P_{10} = P_{12} = \int_{-\infty}^{-T} p(r)\,dr + \int_{T}^{\infty} p(r)\,dr = 1 - P_{00}$$

$$P_{01} = \int_{-T}^{T} p(r - f_{min})\,dr = \frac{1}{2}\mathrm{erf}\left(\frac{T - f_{min}}{\sigma_r\sqrt{2}}\right) - \frac{1}{2}\mathrm{erf}\left(\frac{-T - f_{min}}{\sigma_r\sqrt{2}}\right)$$

$$P_{11} = \int_{-\infty}^{-T} p(r - f_{min})\,dr + \int_{T}^{\infty} p(r - f_{min})\,dr = 1 - P_{01}$$

Equations 4.6 - 4.9

$$\text{where } \int_{\mu-T}^{\mu+T} \mathrm{Gaussian}(\mu,\sigma)\,\partial x = \frac{2}{\sqrt{2\pi\sigma^2}} \int_{\mu}^{\mu+T} \exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right)\partial x = \frac{2}{\sqrt{\pi}} \int_{0}^{T/\sigma\sqrt{2}} \exp(-y^2)\,\partial y = \mathrm{erf}\left(\frac{T}{\sigma\sqrt{2}}\right)$$

An average cost function or risk ($\Re$) is determined for our fault detection scheme:

$$\Re = \sum_{i=0}^{1}\sum_{j=0}^{2} P_j P_{ij} C_{ij}$$

$$= P_0C_{10} + P_1C_{11} + P_2C_{12} + P_1P_{01}(C_{01} - C_{11}) + P_2P_{02}(C_{02} - C_{12}) - P_0P_{00}(C_{10} - C_{00})$$

Equation 4.10

The first three terms represent the fixed cost of our decision and the remaining terms may be minimized with the following relation or likelihood ratio test (LRT):

$$P_1P_{01}(C_{01} - C_{11}) + P_2P_{02}(C_{02} - C_{12}) \underset{\text{say } H_0}{\overset{\text{say } H_1}{\gtrless}} P_0P_{00}(C_{10} - C_{00})$$

$$\frac{P_{01}}{P_{00}} \underset{\text{say } H_0}{\overset{\text{say } H_1}{\gtrless}} \frac{P_0(C_{10} - C_{00}) - P_2(C_{02} - C_{12})}{P_1(C_{01} - C_{11})} = \eta$$

Equation 4.11

The quantity on the left in the above decision rule is called the likelihood ratio, denoted by $\Lambda(r)$, and is determined directly from the conditional pdfs defined above:

$$\Lambda(r) = \frac{P_{01}}{P_{00}} = \frac{p(r - f_{min})}{p(r)} = \exp\left(\frac{r \times f_{min}}{\sigma_r^2} - \frac{f_{min}^2}{2\sigma_r^2}\right)$$

Equation 4.12

The likelihood ratio test for our detection scheme compares the absolute value of the residual to the threshold T and is thus generalized in order to account for a fault in either controller (i.e. any fault $f = |f_1 - f_2| \geq f_{min}$). The threshold T can be directly determined from the above decision rule using the derived form for the likelihood ratio $\Lambda(r)$. The final form for the difference test results upon slight rearrangement of the decision rule:

$$|r| \underset{\text{say } H_0}{\overset{\text{say } H_1}{\gtrless}} T = \frac{\sigma_r^2}{f_{min}} \log\eta + \frac{f_{min}}{2}$$

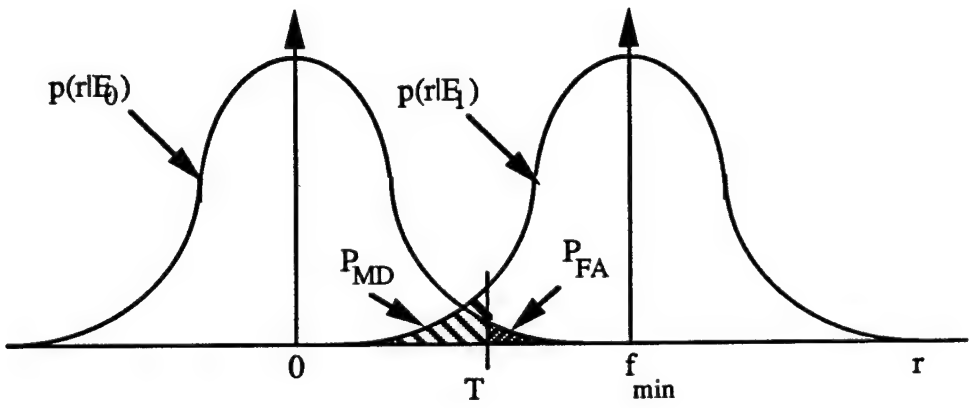
Equation 4.13

A special cost assignment that is frequently encountered in practice (e.g. the cost values cannot be determined directly) is one where correct decisions incur no penalty ($C_{00} = C_{11} = C_{12} = 0$) and incorrect decisions incur the same penalty ($C_{10} = C_{01} = C_{02} = 1$). With this cost assignment, risk is equivalent to the probability of decision error and a simpler definition for η is achieved:

$$\Re = P_{Error} = P_0P_{10} + P_1P_{01} + P_2P_{02} \quad \text{and} \quad \eta = \frac{P_0 - P_2}{P_1} \cong \frac{P_0}{P_1}$$

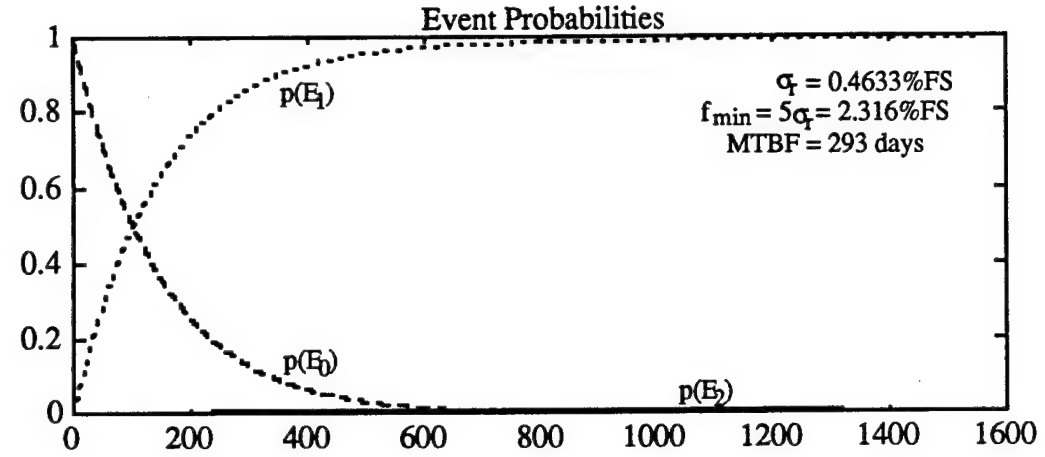
Equations 4.14 and 4.15

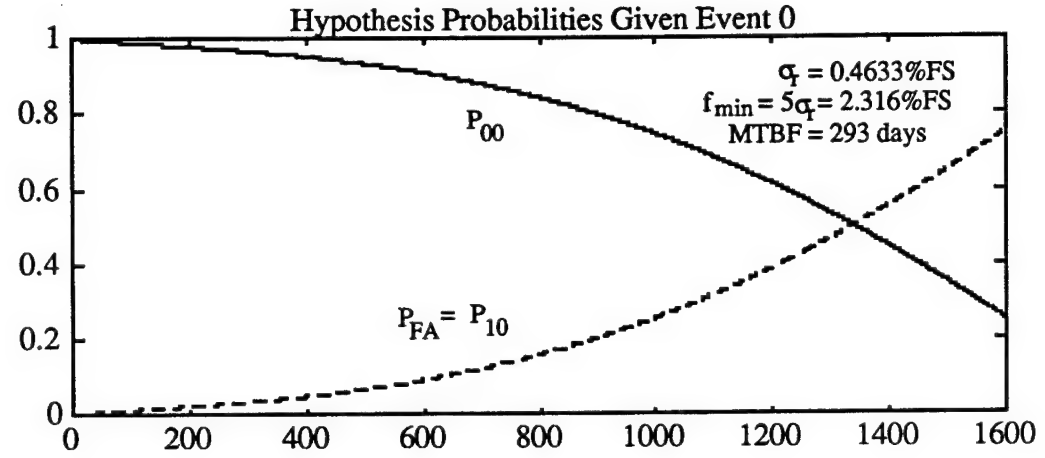
Figures 4.5 - 4.13 provide a perspective on the efficiency of the dual-difference detection scheme based on the Bayes criterion with this special cost assignment. The example error function (σ = 0.3276%FS, Figure 2.4) and the example reliability distribution (MTBF = 293 days, Figure 3.7) for a typical control structure are used. The conditional probability density function of the residual or test function r under both of the primary hypotheses E_0 and E_1 is exemplified in Figure 4.5. This figure provides a perspective on the nature of the two types of decision error and the extent of their probabilities P_{FA} and P_{MD}. Note the dramatic dependence upon the threshold T. Figures 4.6 - 4.11 represent all variables of interest within the dual-difference detection scheme for a fault amplitude $f_{min} = 5\sigma_r$ = 2.3165%FS. Note that the probability of a dual fault $p(E_2)$, false alarm P_{FA}, missed detection P_{MD}, and decision error P_{Error} are very small; while the probability of fault detection P_D is almost completely certain, regardless of when a fault should occur. The threshold T is originally made quite large while the probability of normal operation is high and subsequently is pulled closer towards the origin as the probability of a structure fault increases. Thus, the threshold is varied according to the prior event probabilities of the control structure. Figures 4.12 and 4.13 depict the effect upon the threshold T and the resulting probability of decision error for the fault detection scheme as the ratio of the fault signal f_{min} to the noise deviation σ_r is increased from one-half to five. Worst-case corresponds to a fault magnitude and ratio of zero (i.e. where a fault cannot be distinguished with the residual) and the probability of error is 50% at all times due to the blind guess of either event E_0 or E_1. There is a definite reduction in this probability of decision error with increasing fault signal-to-noise ratio (SNR). Therefore, this analysis is limited to the smallest fault magnitude f_{min} of importance or cost. In addition, this relationship highlights the importance of minimization of the residual noise ($\sigma_r = \sigma\sqrt{2}$) and therefore the error deviation (σ), as detailed in the error budget techniques of Chapter 2, in order to maximize the SNR ratio.

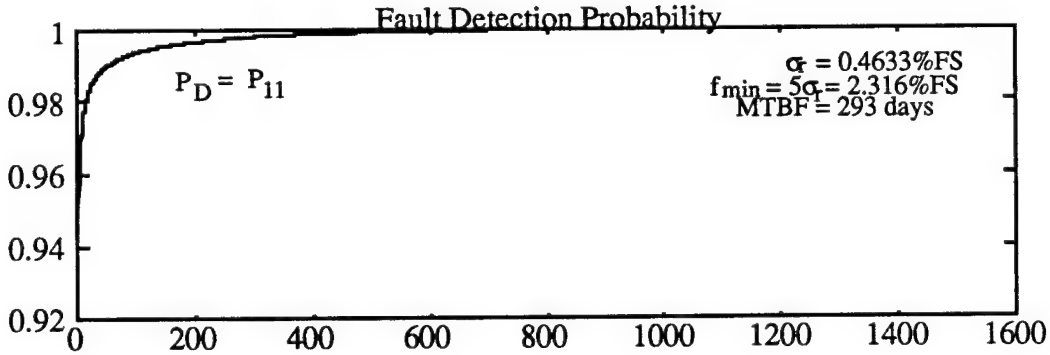


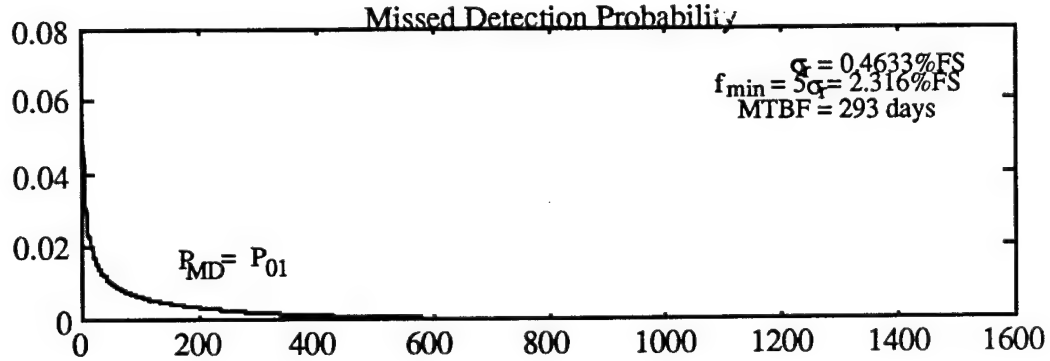
Here, $\eta = \frac{P_0 - P_2}{P_1} > 1$ and thus $T > \frac{f_{min}}{2}$

Figure 4.5 Decision Errors for a Binary Hypothesis Set









Time (Days)

Figures 4.6 - 4.9

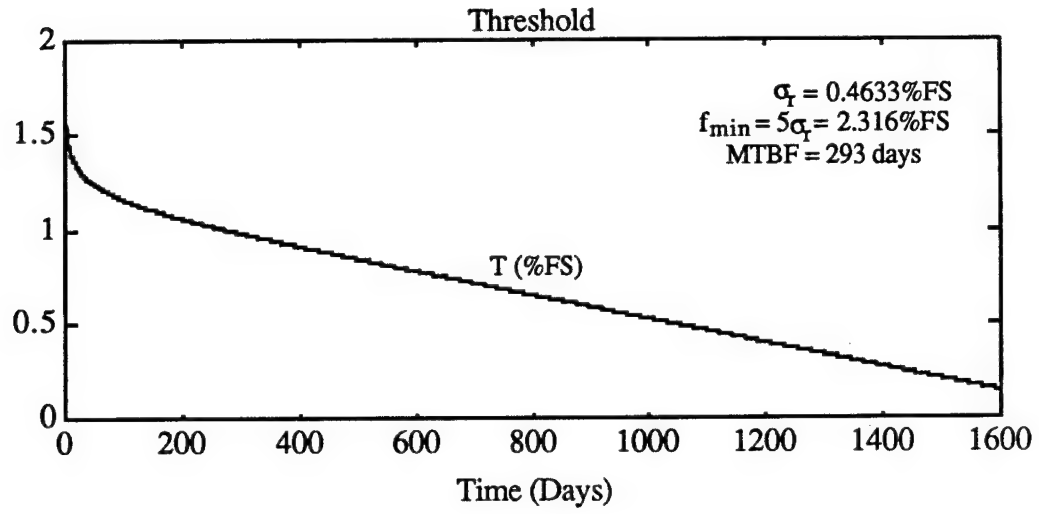


Figure 4.10

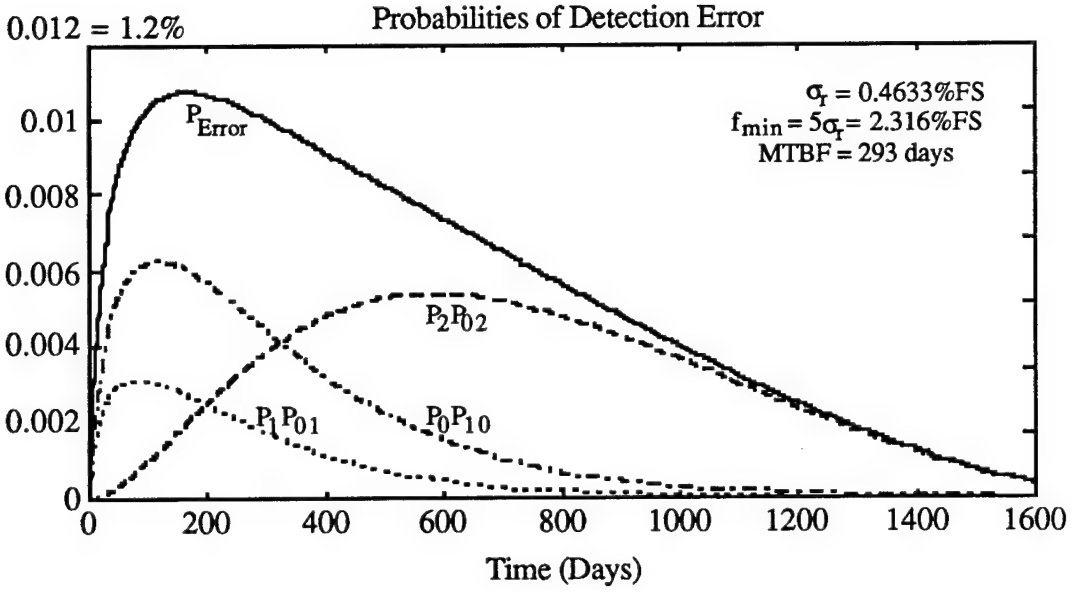


Figure 4.11

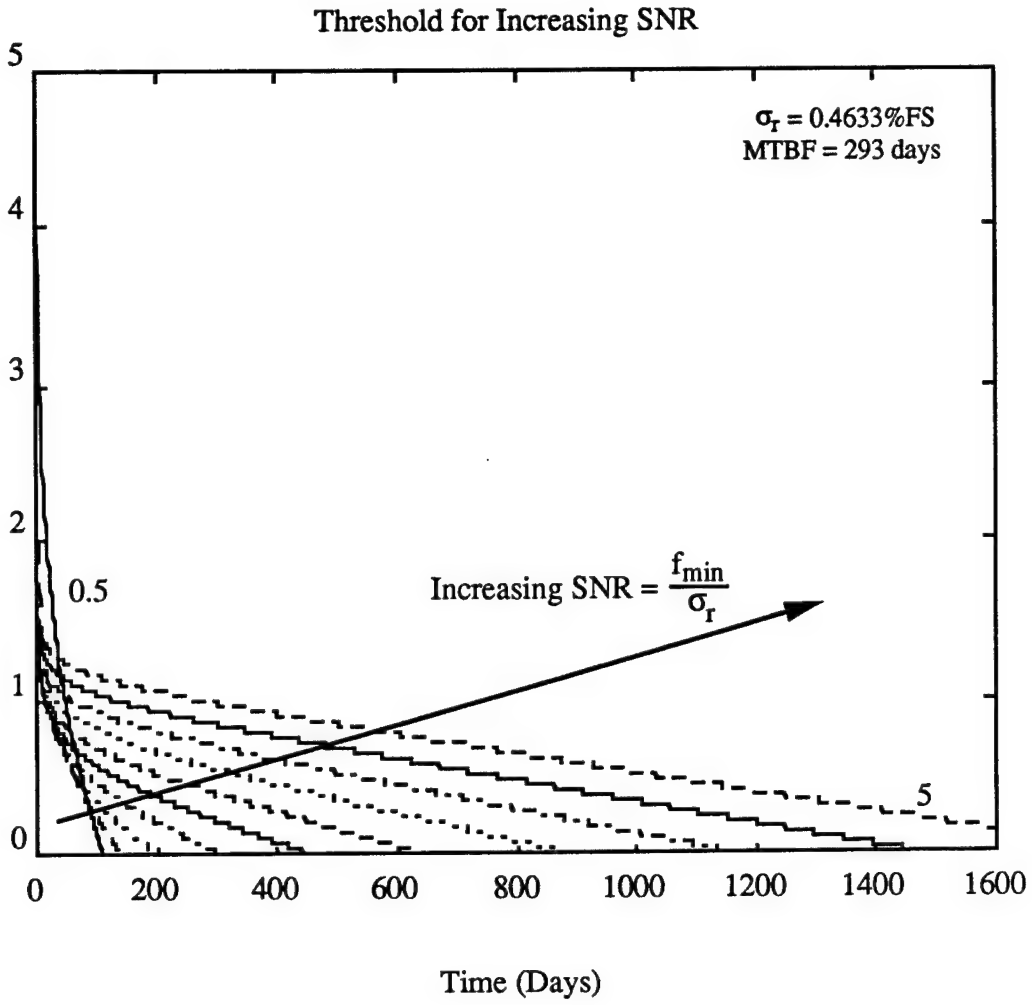

Threshold for Increasing SNR
σ_r = 0.4633%FS
MTBF = 293 days
Increasing SNR = $\frac{f_{min}}{\sigma_r}$
0.5
5
0
1
2
3
4
5
0
200
400
600
800
1000
1200
1400
1600
Time (Days)

Figure 4.12

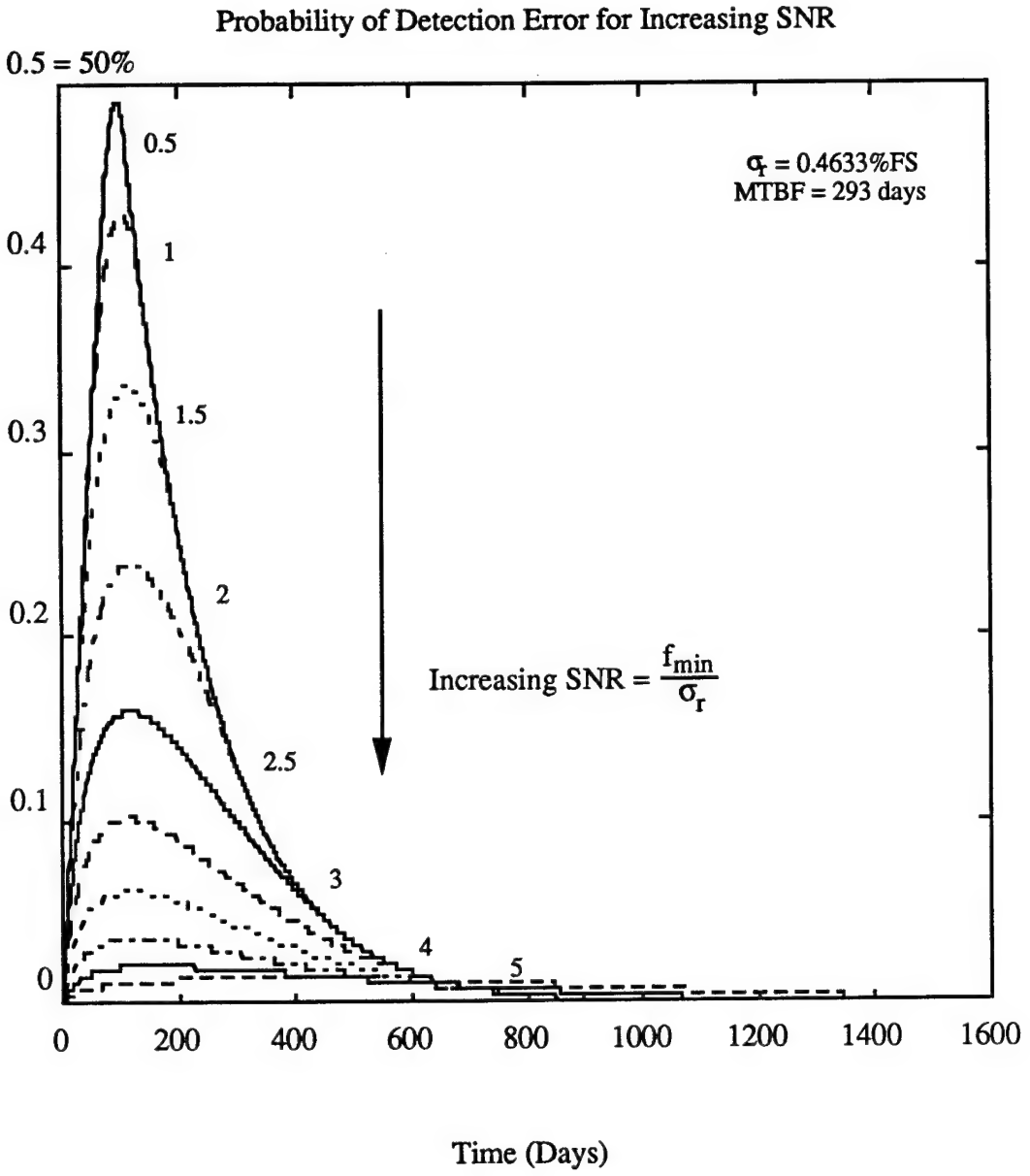

Probability of Detection Error for Increasing SNR
0.5 = 50%
0.4
0.3
0.2
0.1
0
0.5
1
1.5
2
2.5
3
4
5
σr = 0.4633%FS
MTBF = 293 days
Increasing SNR = fmin / σr
0
200
400
600
800
1000
1200
1400
1600
Time (Days)

Figure 4.13

4.3.3. Detection Scheme Optimization with Neyman-Pearson Criterion

Clearly, the objective of any binary hypothesis testing decision algorithm is to achieve very low error probabilities or, equivalently, to simultaneously attain high fault detection P_D and low amount of false alarms P_{FA}. Unfortunately, these goals are in direct conflict with each other in all problems of interest. This problem was not evident within the example of Figures 4.5 - 4.11 due to the large SNR but, in cases dealing with smaller SNR, this problem shall become evident. An explicit means of summarizing the tradeoff between fault detection and false alarms is provided by the receiver operating characteristics (ROC) plot. The ROC plot is merely a graph of P_D vs. P_{FA} and Figure 4.14 represents the Gaussian case analyzed previously. The points $P_{FA} = P_D = 1$ and $P_{FA} = P_D = 0$ are always on the ROC plot because they correspond to the respective strategies of always deciding that a fault has occurred (event E_1) or that the control structure is operative (event E_0). The ROC for any possible test always lies above the dotted line which represents the worst-case scenario of equal priors ($p(E_0) = p(E_1)$) and a strategy of pure guessing without regard to the observations (i.e. the residual). The monotonicity of the ROC plot reflects the fact that fault detection cannot be increased without a subsequent increase in false alarms for a given fault SNR. An obvious criterion is to constrain one of these conditional probabilities while maximizing (or minimizing) the other. As opposed to the Bayes criterion, the Neyman-Pearson criterion recognizes this basic asymmetry in the importance of these two hypotheses. [Poor, Van Trees]

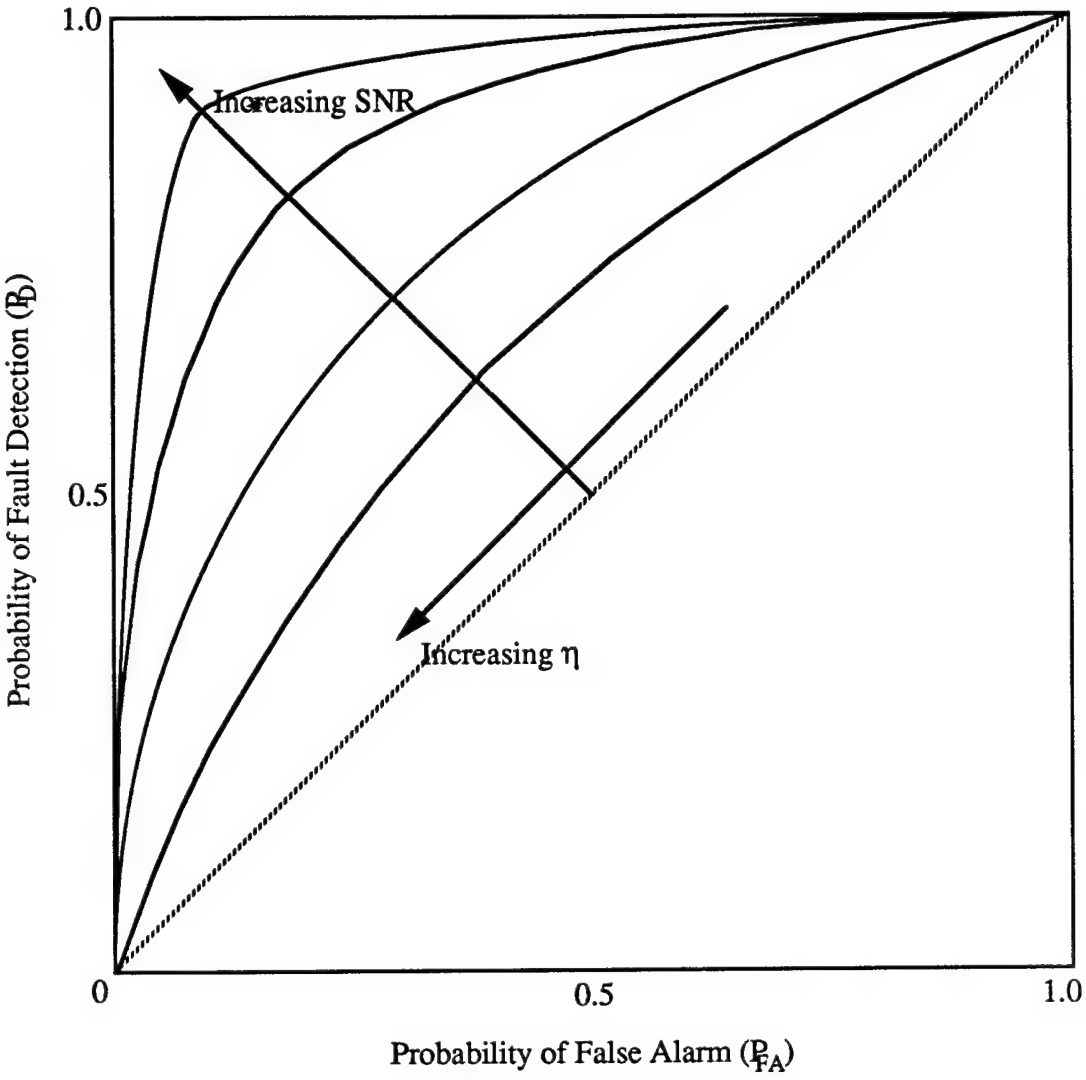


Figure 4.14 Receiver Operating Characteristics (ROC) Plot

The classical Neyman-Pearson criterion of radar detection theory constrains the conditional probability of false alarms P_{FA} to remain less than some arbitrarily small value α, known as the level or significance level of the test, and then maximizes the conditional probability of fault detection P_D to some value $(1-\beta)$, known as the power of the test. This generally assumes that η, known as the threshold of the test, is greater than unity. For example, the cost of false alarms C_{10} could greatly exceed the cost of missed detections C_{01} or the a priori probability of a fault $P_0 = p(E_0)$ might be substantially smaller than that of normal operation $P_1 = p(E_1)$. Since the probability of fault detection monotonically increases with the probability of false alarms (Figure 4.14), maximization of P_D corresponds with a P_{FA} set at its upper bound of α.

$$P_{FA} = P_{10} = \int_{-\infty}^{-T} p(r)\,dr + \int_{T}^{\infty} p(r)\,dr = 1 - \mathrm{erf}\left(\frac{T}{\sigma_r\sqrt{2}}\right) = 1 - \mathrm{erf}\left(\frac{T}{2\sigma}\right) = \alpha$$

$$T = 2\sigma\,\mathrm{erf}^{-1}(1-\alpha) \quad \text{where } \mathrm{erf}^{-1}(x) \text{ is the inverse function of } \mathrm{erf}(x)$$

$$P_D = P_{11} = 1 - \frac{1}{2}\mathrm{erf}\left(\mathrm{erf}^{-1}(1-\alpha) - \frac{f_{min}}{2\sigma}\right) - \frac{1}{2}\mathrm{erf}\left(-\mathrm{erf}^{-1}(1-\alpha) - \frac{f_{min}}{2\sigma}\right) = 1 - \beta$$

Equations 4.16 - 4.18

The threshold T is held constant by the Neyman-Pearson criterion and it is completely defined by Equation 4.17 upon choosing the level of the test (α). Likewise, the power of the test is held constant and is defined by Equation 4.18, known as the power function of the test. The power of the test (fault detection) is a monotonic function of the level of the test (false alarms) and a change in one implies our willingness to accept a similar change in the other. Note that decision costs are not evaluated and the prior event probabilities are not incorporated within the Neyman-Pearson criterion and, thus, this information is forfeited for a simpler approach to the fault detection scheme.

Figures 4.15 - 4.17 provide a perspective on the efficiency of the dual-difference detection scheme based on the Neyman-Pearson criterion. The example error function (σ = 0.3276%FS, Figure 2.4) and the example reliability distribution (MTBF = 293 days, Figure 3.7) for a typical control structure are used. Figures 4.15 - 4.16 represent all variables of interest within the dual-difference detection scheme for a fault amplitude f_{min} = $5\sigma_r$ = 2.3165%FS with the threshold set at a constant three sigma interval ($T = 3\sigma_r$). Therefore, the level of the test (probability of false alarms, P_{FA}) is 0.27% and the power of the test (probability of fault detection, P_D) is 97.72%. Note that the probability of decision error P_{Error} is very small, while the probability of fault detection P_D is very certain regardless of when a fault should occur. In comparison with the performance of the fault detection scheme based on the Bayes criterion at a SNR of five, the Neyman-Pearson criterion allows for a similar level of decision error with a reduction in the design complexity. However, an increase is found to occur in the probability of missed detection of a dual fault (event E_2). Figure 4.17 depicts the resulting probability of decision error for the fault detection scheme as the ratio of the fault signal f_{min} to the noise deviation σ_r is increased from one-half to five. Analysis of Figure 4.17 indicates that a large fault signal-to-noise ratio is required to even warrant using the Neyman-Pearson criterion for the fault detection scheme. For small SNR ratios, the 3σ setting for the threshold hides the fault distribution from the test (corresponding to always deciding event E_0) and the probability of error approaches 100% as the reliability approaches zero at long mission times. Worst-case for the Bayes criterion corresponds to an SNR of zero (i.e. where a fault cannot be distinguished with the residual) and the probability of error is 50% at all times due to the blind guess of either event E_0 or E_1. Note that all curves in Figure 4.17 exhibit the exponential rise associated with the unreliability because the threshold is not adjusted (as it is with the Bayes criterion) to account for changes in the prior distributions. Also, there is a definite reduction in this probability of decision error with increasing fault signal-to-noise ratio (SNR).

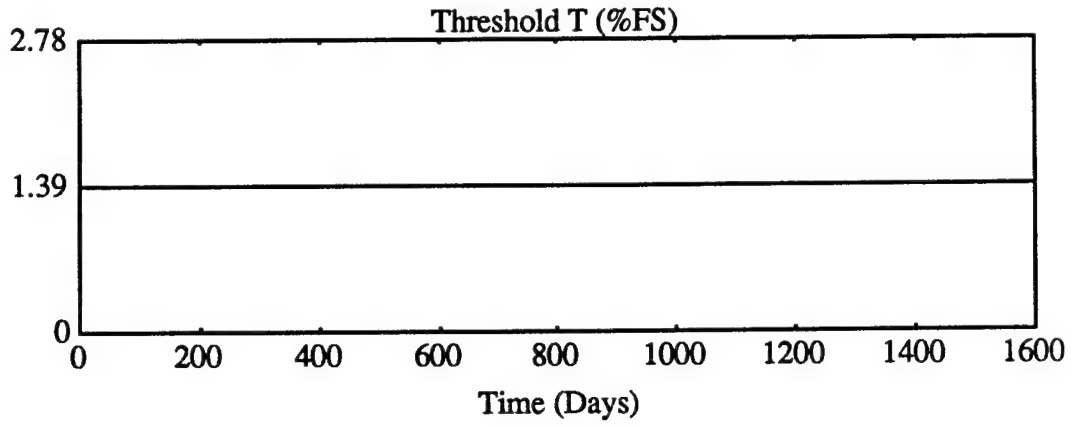


Figure 4.15

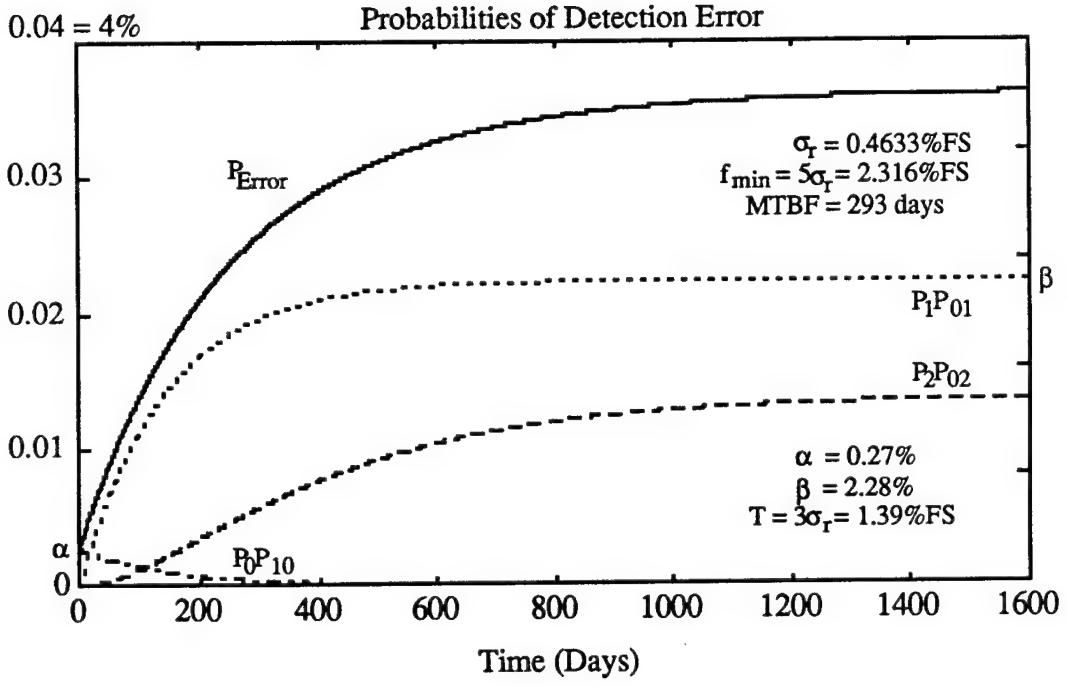


Figure 4.16

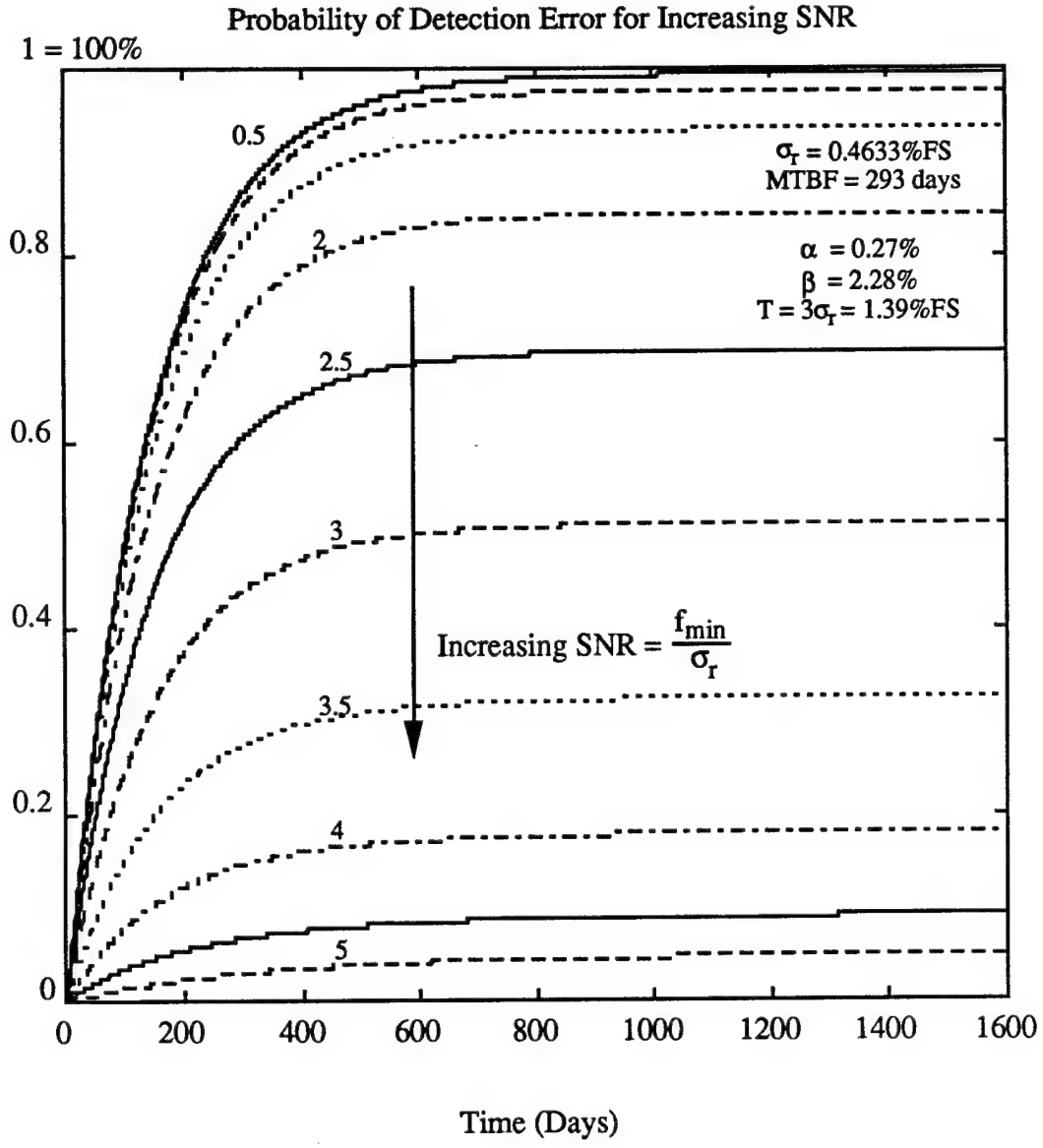

Probability of Detection Error for Increasing SNR
1 = 100%
0.8
0.6
0.4
0.2
0
0.5
2
2.5
3
3.5
4
5
σr = 0.4633%FS
MTBF = 293 days
α = 0.27%
β = 2.28%
T = 3σr = 1.39%FS
Increasing SNR = fmin / σr
0
200
400
600
800
1000
1200
1400
1600
Time (Days)

Figure 4.17

4.3.4. Duplex Fault Isolation and Reconfiguration

Upon fault detection within the control structure, diagnostic schemes must be initiated to isolate the failed structure(s), locate and report the faulty module(s), and reconfigure the system in order to provide continuous valid control for the length of the mission (Note: system shutdown is not considered possible in this exercise!). The dual nature of the DDRS afforded quick and efficient validation of the controllers with the difference test. However, no new information may be gained by further comparison of the two structures once a fault has been detected. Hence, subsequent decisions must be based on further analysis of the individual controllers (simplex FDI, Section 4.2). Otherwise, either controller may be decided as valid with a 50% chance of correct isolation (flip a coin) given that a single fault has occurred and with complete error upon occurrence of a dual fault. In this case, note that the probability of misisolation by blind guess given that a fault has been detected (Equation 4.19) goes to unity as time goes to infinity. Reconfiguration consists of removing the faulty controller from the output estimation scheme (i.e. averaging) yet still including it as a voter in the FDI scheme. The faulty controller is simply returned to valid status upon a successful difference test. This reconfiguration scheme allows recovery from false alarms and transient faults and maintains the independence between successive difference tests of the DDRS over the mission. Alternatively, reconfiguration may consist of ignoring the faulty controller's output in all future operations (Section 4.5) with the final possible state of the system being shutdown. Figure 4.18 depicts the decision tree associated with our FDI scheme for two levels of redundancy where correct decisions are denoted with a check mark. The probability of each possible system state can be directly determined from the decision tree (Equations 4.20 - 4.24). Figure 4.19 follows the total probability of decision error for the FDI scheme over the mission time of our example control structure, accounting for both: detection errors based on the Bayes criterion; and isolation errors by blind guess. Due to the near optimality of

the detection scheme in this example (i.e. $P_{00} = P_{11} = 1$), P_{Error} (Equation 4.25) is approximately the probability of misisolation by blind guess (Equation 4.19).

$$\Pr\{\text{Misisolation} \mid \text{Fault Detected}\} = (1 - \Pr\{\text{Isolation} \mid f_1,f_2\})\Pr\{f_1,f_2\} + (1 - \Pr\{\text{Isolation} \mid f_1\})\Pr\{f_1\} + (1 - \Pr\{\text{Isolation} \mid f_2\})\Pr\{f_2\}$$

$$\Pr\{\text{Misisolation by Blind Guess} \mid \text{Fault Detected}\} = 2\,(0.5)\,R_S(t)\,Q_S(t) + Q_S^2(t)$$

(Equation 4.19)

Probability of Each Possible System State for the DDRS

$$P_{S1} = R_S^2 P_{00};\quad P_{S2} = 2\,Q_S\,R_S\,P_{01};\quad P_{S3} = Q_S^2\left(\frac{A_{DT}}{FS^2}\right)P_{00} + Q_S^2\left(1 - \frac{A_{DT}}{FS^2}\right)P_{01};$$

$$P_{S4} = R_S^2 P_{10} + Q_S\,R_S\,P_{11};\quad P_{S5} = Q_S^2\left(\frac{A_{DT}}{FS^2}\right)P_{10} + Q_S^2\left(1 - \frac{A_{DT}}{FS^2}\right)P_{11} + Q_S\,R_S\,P_{11}$$

Equations 4.20 - 4.24

States

1: Dual Structure,Both Working
2: Dual Structure,One Working
3: Dual Structure,None Working
4: Single Structure,Working
5: Single Structure,Not Working

Probability of System Error for the DDRS

$$P_{Error} = P_{S2} + P_{S3} + P_{S5} + R_S^2 P_{10} = Q_S^2 + Q_S\,R_S\,P_{11} + 2\,Q_S R_S\,P_{01} + R_S^2 P_{10}$$

$$= Q_S^2 + Q_S\,R_S \quad \text{for the optimal fault detection scheme} \qquad \text{(Equation 4.25)}$$

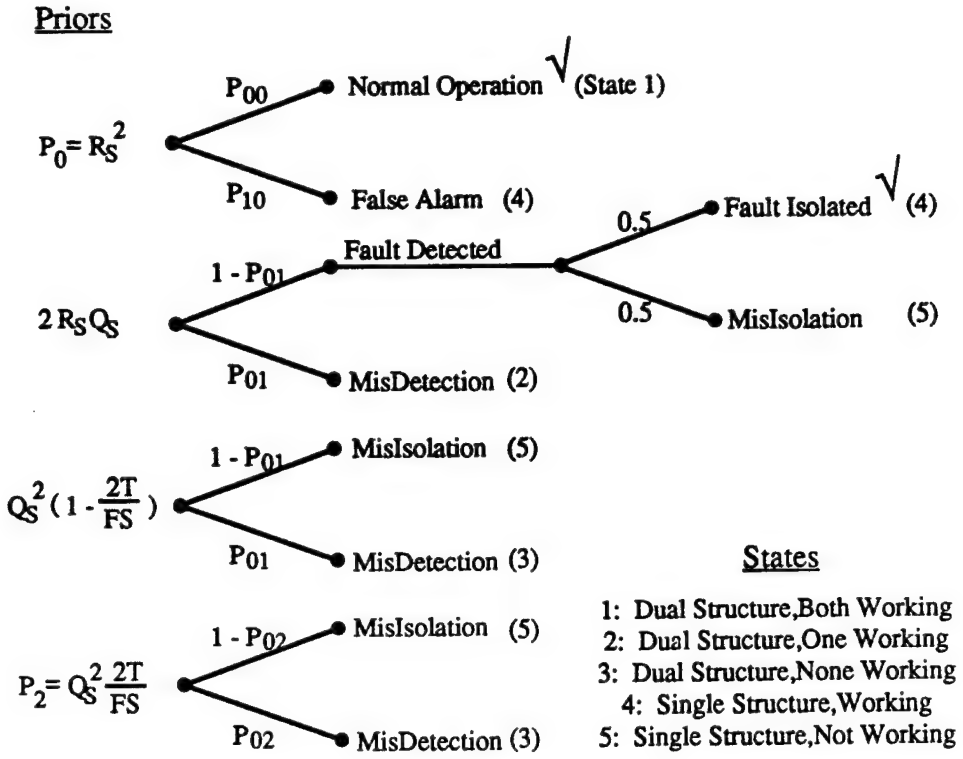


Figure 4.18 Decision Tree for FDI Scheme with Dual Redundancy

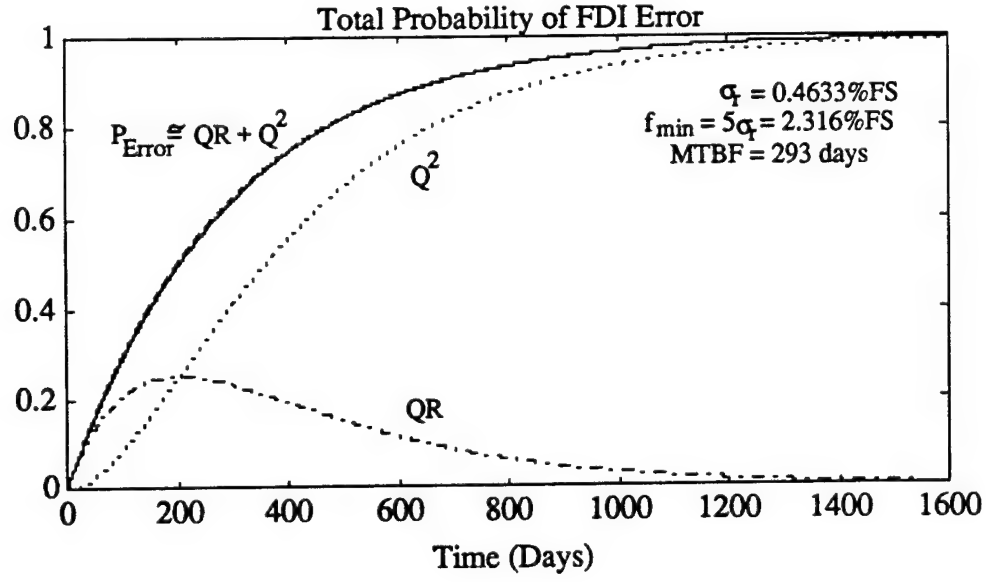


Figure 4.19 Probability of Decision Error for Optimal FDI Scheme

4.4. Triplex Fault Detection and Isolation

With triple modular redundancy (TMR), structure validation is provided by comparison of three identical control structures. TMR is actually the most common form of traditional majority-voting schemes. Its obvious advantage over dual redundancy is the efficient means of isolating a single structure fault . . . a direct extension of the DDRS to allow for fault-tolerant control of the system. Additionally, unreliability and error are reduced with each level of redundancy. Entropy, however, is increased with redundancy. Upon fault detection and isolation, the triplex system reconfigures to the DDRS utilizing the two valid controllers. The benefits of a triplex system are lost during a common dual or triple fault and perhaps even become a detriment if the voting scheme follows the faulty controllers. However, as seen before, the probability of a common fault is small. Finally, the additional hardware requires more expense and working volume per system variable than might be afforded. Space limitations is one of the major reasons current fault-tolerant techniques have shifted their attention to analytical redundancy (i.e. system models).

4.4.1. Two-dimensional Parity Space

The combination of a triple redundant control structure (TRS) and probabilistic models of the structure error and reliability allows for an efficient method of: 1) validation of triple controller performance, 2) isolation of a single controller fault, and 3) reconfiguration to the DDRS. Comparison tests of the controller signals detect and isolate faults by observing disagreements in controller demands. A sufficient statistic for these comparison tests must be defined which: 1) is a linear combination of controller signals (e.g. input sensor measurements), and 2) removes the unknown controller variable (u) and error mean (μ_ε), common to all signals, from the test. The latter property allows the use of a comparison threshold determined a priori that is dependent upon the signal-to-noise ratio (SNR) of structure error deviation (σ) and the smallest fault magnitude of accountable cost

(f_{min}). As seen in the previous section, a simple difference between controller variables can validate DDRS operation. However, the set of three difference equations possible for the TRS is linearly dependent and does not facilitate a probabilistic analysis of the FDI scheme. For an n-dimensional parameter space, only a set of (n-1) independent linear comparison tests can be derived because each comparison test must include at least two parameters to remove the controller variable. Hence, a two-dimensional parity or comparison space (Figure 4.20) composed of two parity equations (Equations 4.26, 4.27) is suggested by Walker to facilitate fault detection and isolation for the TRS. [Walker]

Parity Vector $\underline{p}$: $$p_1 = \frac{2}{\sqrt{6}}u_1 - \frac{1}{\sqrt{6}}u_2 - \frac{1}{\sqrt{6}}u_3 \qquad \text{(Equations 4.26, 4.27)}$$

$$p_2 = \frac{1}{\sqrt{2}}u_2 - \frac{1}{\sqrt{2}}u_3$$

Parity Vector $\underline{p}$: $$r = \sqrt{p_1^2 + p_2^2} \; ; \quad \theta = \tan^{-1}\left(\frac{p_2}{p_1}\right) \qquad \text{(Equations 4.28, 2.29)}$$

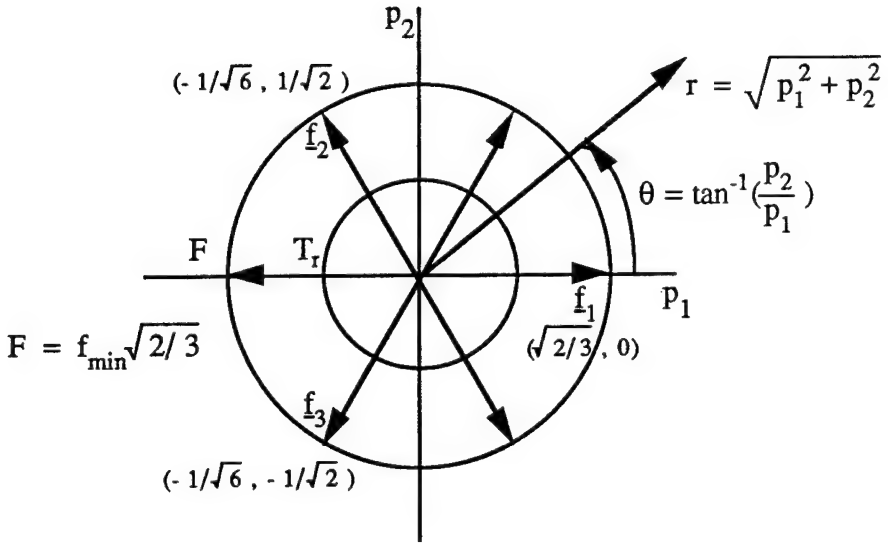


Figure 4.20 Two-Dimensional Parity Space for the TRS

Equations 4.26 and 4.27 define the two orthonormal residuals which comprise the two-dimensional parity space for the triple redundant control structure. Orthonormality dictates that: 1) the residuals are orthogonal (i.e. perpendicular) and thus retain a zero mean, and 2) each residual is normalized to a unit vector of unity magnitude. Further, this orthonormal set of parity equations corresponds to a 2 x 3 linear transformation matrix P of the controller signals comprised of the eigenvectors of the 3 x 3 diagonal correlation matrix A of the parameter space. This transfers the uncorrelated Gaussian distribution with zero means and equal variances of the parameter space to the parity space (diagonal correlation matrix D):

$$P = \begin{bmatrix} \frac{2}{\sqrt{6}} & \frac{-1}{\sqrt{6}} & \frac{-1}{\sqrt{6}} \\ 0 & \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{bmatrix} \qquad P^{-1} = P^{T} = \begin{bmatrix} \frac{2}{\sqrt{6}} & 0 \\ \frac{-1}{\sqrt{6}} & \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{6}} & \frac{-1}{\sqrt{2}} \end{bmatrix} \qquad A = \begin{bmatrix} \sigma^2 & 0 & 0 \\ 0 & \sigma^2 & 0 \\ 0 & 0 & \sigma^2 \end{bmatrix}$$

Theorem For every n x n real symmetric matrix A there exists an m x n ($m \leq n$) real orthogonal matrix P such that $PAP^{-1} = D$, or, equivalently, such that $PAP^{T} = D$, where D is a diagonal matrix. [Bronson]

Here,

$$D = PAP^{-1} = P\,\sigma^2 I_3\, P^{-1} = \sigma^2 I_2 \quad \text{where } I_n = n \text{ x } n \text{ identity matrix}$$

The resultant two-dimensional parity space is depicted in Figure 4.20. The goal of this parity vector approach is to generate signals which are insensitive to modelling errors, highly sensitive to failures, and respond to different failures in easily recognized ways to facilitate isolation. Neglecting error terms, the fault signatures of the three controllers are defined by three distinct and equidistant vectors ($\underline{f}_1$, $\underline{f}_2$, and $\underline{f}_3$, respectively) of equal

magnitude F and their three corresponding inverses which split the plane into six equal pieces. Our fault detection scheme takes advantage of this balanced or symmetrical property of uniform detectability by utilizing a circular threshold of radius T_r as a comparison test against the radius r of the parity vector. Our fault isolation scheme divides the parity space into six equal pie sections of 60^o each and centers them about each of the three fault signatures and their inverses. Hence, the parity space is also further transformed to polar coordinates of radius r and angle θ (Equations 4.28,4.29). The definition of full scale magnitude (FS) corresponds to an additional, outermost circle in the parity space which confines the parity vector for all time. [Gai,Weber]

The drawback of this comparison test is that our detection scheme is also insensitive to certain combinations of concurrent faults; specifically, a dual or triple fault where the resultant fault vector ($\underline{f}$) lies within the circular threshold T_r (A blind spot, if you will). Where one fault alone might be of significant magnitude to pass beyond the circular threshold and hence be observable by the comparison test, the resultant fault vector in the parity space (as determined by Equations 4.26, 4.27) cancels this effect and the faults become hidden from the test. The probability of a hidden dual fault or hidden triple fault are determined below for small threshold T_r (Equations 4.30, 4.31). A uniform, equivalent fault distribution is assumed for all controllers (the faults have an equal chance of achieving any magnitude up to full scale and, therefore, a fault vector has an equal chance of reaching any point in the error space). The probability of the occurrence of a hidden fault can be based on the ratio of the area of possible hidden fault vectors (as depicted in Figures 4.21 and 4.22) to the total area of possible fault vectors in the three-dimensional fault space. Note the resemblance of the area of possible dual hidden fault vectors (Figure 4.21) to the hidden space of the difference test for the DDRS (Figure 4.3). The following analysis is only valid for small threshold T_r because it does not account for limiting effects to the area of possible hidden fault vectors near the fullscale (FS) values of the fault space.

Probability of a Hidden Dual Fault in TRS (given that a dual fault has occurred)

Without Loss of Generality (WOLOG), assume $f_1 = 0$.

$$\Pr\{ \text{Hidden Dual Fault} \mid f_2 \,\&\, f_3 \text{ Dual Fault}, f_1 = 0 \} = \Pr\{ r = \sqrt{p_1^2 + p_2^2} \le T_r \mid f_2 \,\&\, f_3 , f_1 = 0 \}$$

$$= \Pr\{ \mid f_2^2 + f_3^2 - f_2 f_3 \mid \le \tfrac{3}{2} T_r \} = \frac{3 (\sqrt{\tfrac{3}{2}}\, T_r)^2}{(2\,FS)^2} = \frac{9\,T_r^{\,2}}{8\,FS^2}$$

$$\Pr\{ \text{Hidden Dual Fault} \mid \text{TRS Dual Fault} \} = \frac{9\,T_r^{\,2}}{8\,FS^2} \qquad \text{(Equation 4.21)}$$

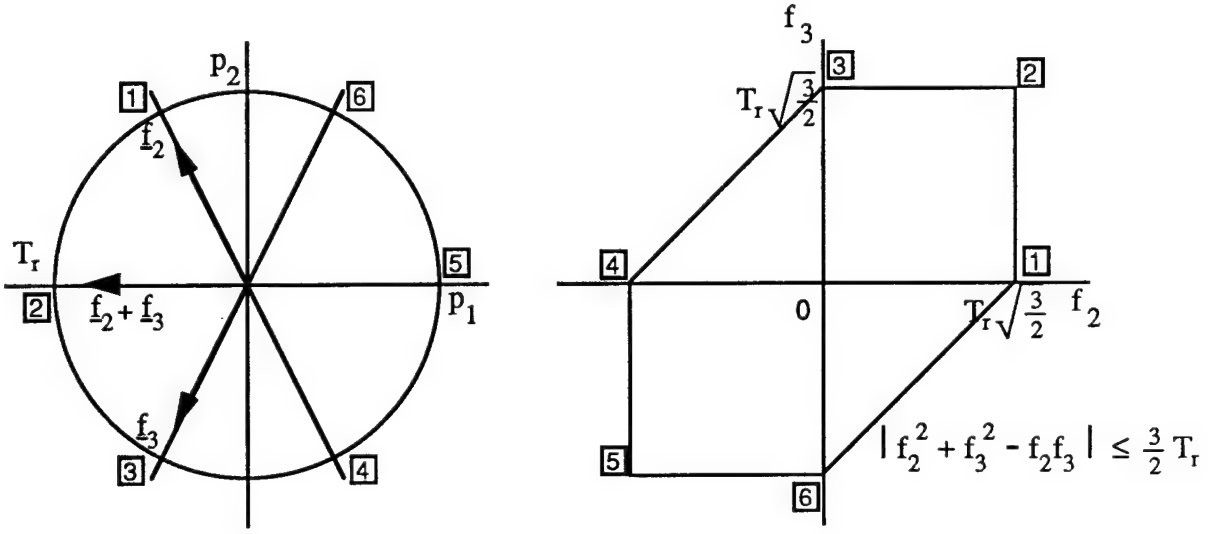


Figure 4.21 Hidden Dual Fault Represented in Parity and Fault Spaces

Probability of a Hidden Triple Fault in TRS (given that a triple fault has occurred)

$$\Pr\{\text{ Hidden Triple Fault} \mid f_1 \,\&\, f_2 \,\&\, f_3 \text{ Triple Fault }\} = \Pr\{ r = \sqrt{p_1^2 + p_2^2} \le T_r \mid f_1 \,\&\, f_2 \,\&\, f_3 \}$$

$$= \Pr\{ \mid f_1^2 + f_2^2 + f_3^2 - f_1 f_2 - f_1 f_3 - f_2 f_3 \mid \le \tfrac{3}{2} T_r \} = \frac{(2 + \frac{1}{3})(\sqrt{\frac{3}{2}}\, T_r)^3}{(2\,FS)^3} = \frac{7\sqrt{3}\; T_r^{\,3}}{16\sqrt{2}\, FS^3}$$

$$\Pr\{\text{ Hidden Triple Fault} \mid \text{TRS Triple Fault }\} = \frac{7\sqrt{3}\; T_r^{\,3}}{16\sqrt{2}\; FS^3} \qquad \text{(Equation 4.22)}$$

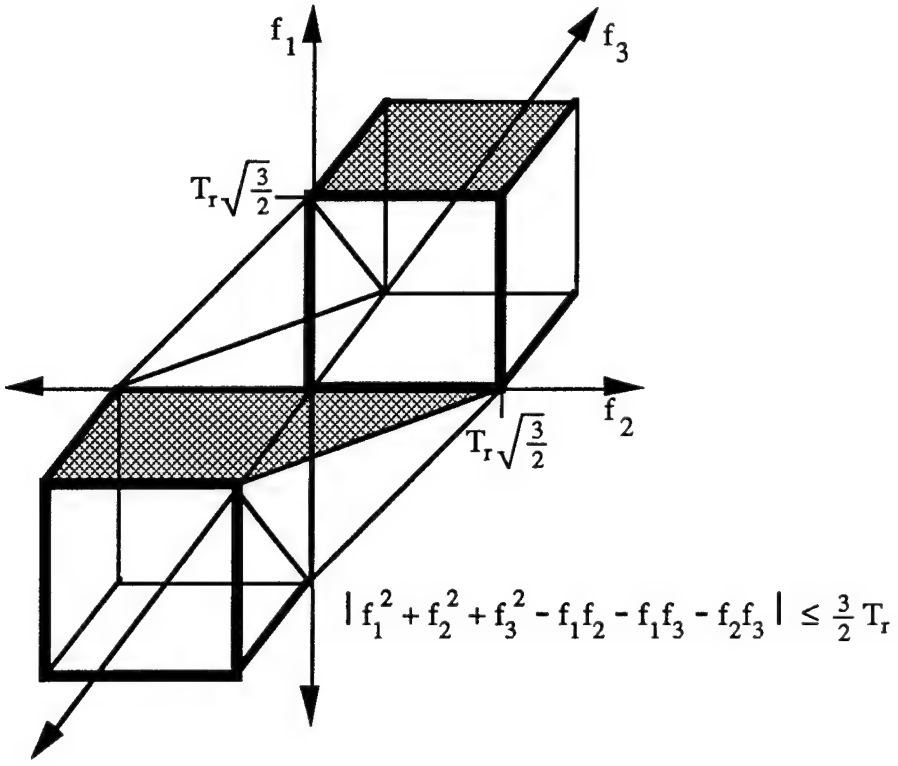


Figure 4.22 Hidden Triple Fault Represented in the Fault Space

4.4.2. Detection Scheme Optimization with Bayes Criterion

Our fault detection scheme is analyzed as a classical, M-ary hypothesis test (M=4) with a fixed, singular data sample. [Van Trees] With each sample, it is assumed that a decision from M possible decisions must be made as to which event of M possible events has occurred. Thus, there are M possible alternatives or event-hypothesis pairings each time a decision must be made. The four events E_0, E_1, E_2, and E_3 in our fault detection scheme are that no fault, a single fault, or a hidden fault of dual or triple nature has occurred, respectively. Our decision will be facilitated by a unique physical manifestation associated with each event (i.e. the magnitude with which each event affects the measurable parity vector $\underline{p}$). Dual and triple faults other than a hidden fault are assumed to be indistinguishable from single structure faults with respect to the threshold test and are, therefore, included in event E_1. This fact has important ramifications in our attempt to isolate a fault to the structure in which the fault occurred. Event E_1 is represented as an additive fault vector of magnitude F (Figure 4.20) which causes the parity vector to shift outside the circular threshold T_r. This analysis is concerned with the worst-case magnitude of f (f_{min}) which is the smallest fault (and, thus, the hardest to detect) of accountable cost for the current application. A major concern is that event E_2 and E_3 (hidden faults) have no effect on the parity vector and cannot be distinguished from normal operating conditions.

$$P_0 = p(E_0) = R_S^3(t);\quad P_2 \cong 3\,R_S(t)\,Q_S^2(t)\,\frac{9\,T_r^{\,2}}{8\,FS^2};\quad P_3 \cong Q_S^3(t)\,\frac{7\sqrt{3}\;T_r^{\,3}}{16\sqrt{2}\;FS^3};\quad P_1 = 1 - P_0 - P_2 - P_3$$

Equations 4.23 - 4.26

Our fault detection scheme is optimized by using a generalized likelihood ratio test (GLRT) which is based on a degenerated Bayes criterion. [Van Trees] The Bayes criterion assumes the a priori determination of the event probabilities, the conditional probabilities for each decision given the occurrence of each event, and the costs associated with each possible event-hypothesis pairing. For this exercise, the Bayes criterion is degenerated such that only two hypotheses are of importance (H_0 = valid performance, H_1 = fault detected) and only eight alternate pairings are possible.

An average cost function or risk ($\Re$) is determined for our fault detection scheme and is minimized with the likelihood ratio test (LRT). The special cost assignment where correct decisions incur no penalty and incorrect decisions incur the same penalty is utilized. With this cost assignment, risk is equivalent to the probability of decision error. The likelihood ratio, denoted by $\Lambda(r)$, is determined directly from the ratio of the envelope's marginal densities under either event. The resultant test for our detection scheme compares the radius r to the derived threshold T_r and is thus generalized in order to account for a fault in any controller.

The following analysis draws heavily upon the theory of envelope detection used quite commonly in radio communications and radar. [Schwartz, Peebles, Shanmugam] We shall first consider the case of normal operating conditions where only noise is present (i.e. Event 0). Recall from Section 4.2.1. that the components of the parity vector (p_1 and p_2) are Gaussian, uncorrelated, and hence statistically independent. Further, these parameters were transformed to polar coordinates (r and θ) and the Jacobian of this transformation is readily found to be the radius r (i.e. $dx\,dy = r\,dr\,d\theta$). The probability distributions for these variables are as follows:

$$p(p_1, p_2 | E_0) = \frac{1}{2\pi\sigma^2} \exp\left(-\frac{(p_1^2 + p_2^2)}{2\sigma^2}\right) = \frac{1}{2\pi\sigma^2} \exp\left(-\frac{r^2}{2\sigma^2}\right)$$

$$p(r,\theta | E_0) = \frac{r}{2\pi\sigma^2} \exp\left(-\frac{r^2}{2\sigma^2}\right)$$

(Equations 4.27, 4.28)

To find the marginal density functions for the envelope and phase alone, we simply average the joint density function over all possible values for the angle and radius, respectively:

$$p(r | E_0) = \int_0^{2\pi} p(r,\theta | E_0)\, \partial\theta = \frac{r}{\sigma^2} \exp\left(-\frac{r^2}{2\sigma^2}\right); \quad p(\theta | E_0) = \int_0^{\infty} p(r,\theta | E_0)\, \partial r = \frac{1}{2\pi}$$

(Equations 4.29, 4.30)

The marginal density of the envelope is the Rayleigh distribution which is limited to positive values (shown in Figure 4.23 as $F/\sigma = 0$). The conditional probability of false alarm ($P_{10} = P_{FA}$) is easily found to be:

$$P_{FA} = P_{10} = \int_{T_r}^{\infty} p(r | E_0)\, \partial r = -\exp\left(-\frac{r^2}{2\sigma^2}\right)\Big]_{T_r}^{\infty} = \exp\left(-\frac{T_r^2}{2\sigma^2}\right) = 1 - P_{00}$$

(Equation 4.31)

Next, we shall consider the case of a fault condition where a fault vector $\underline{f}$ of magnitude F is present (i.e. Event 1). The components of the fault vector will be denoted f_1 and f_2. The probability distributions for the parity vector and its transform are as follows:

$$p(p_1, p_2 | E_1) = \frac{1}{2\pi\sigma^2} \exp\left(-\frac{(p_1 - f_1)^2 + (p_2 - f_2)^2}{2\sigma^2}\right) = \frac{1}{2\pi\sigma^2} \exp\left(-\frac{r^2 - 2p_1f_1 - 2p_2f_2 + F^2}{2\sigma^2}\right)$$

$$p(r, \theta | E_1) = \frac{r}{2\pi\sigma^2} \exp\left(-\frac{r^2 - 2rf_1\cos\theta - 2rf_2\sin\theta + F^2}{2\sigma^2}\right)$$

(Equations 4.32, 4.33)

The conditional probability of missed fault detection ($P_{01} = P_{MD}$) is more difficult to solve. The probability of missing any of the fault signatures ($\underline{f}_1$, $\underline{f}_2$, and $\underline{f}_3$) is equal for all three cases due to the symmetry of the fault signatures and the balanced nature of the Gaussian parity vector. Also, the prior probabilities of any of the three faults occurring are equal (i.e. 1/3). Hence, P_{MD} is equal to the probability of missing any one of the three fault signatures. We shall restrict the analysis to only one of the three possible fault signatures: specifically, a fault on controller one ($\underline{f}_1$) where $f_1 = F$ and $f_2 = 0$. The marginal density function for the envelope is found by averaging the joint density function over all possible angles:

$$p(r \mid \underline{f}_1) = \int_0^{2\pi} p(r, \theta \mid \underline{f}_1)\, \partial\theta = \frac{r}{2\pi\sigma^2} \exp\left(-\frac{r^2 + F^2}{2\sigma^2}\right) \int_0^{2\pi} \exp\left(\frac{r F \cos\theta}{\sigma^2}\right) \partial\theta$$

$$p(r \mid \underline{f}_1) = \frac{r}{\sigma^2} \exp\left(-\frac{r^2 + F^2}{2\sigma^2}\right) I_0\left(\frac{r F}{\sigma^2}\right)$$

(Equation 4.34)

The integral in Equation 4.34 cannot be evaluated in terms of elementary functions but is found to be equivalent to the modified Bessel function of the first kind and zero order $I_0(z)$. [Schwartz] This marginal distribution for the envelope is often called the Rician or Rice distribution (Figure 4.23 by Peebles) in honor of S. O. Rice of Bell Telephone Laboratories who developed and discussed the properties of this distribution in a pioneering series of papers on random noise. [Rice] The Rician distribution is equivalent to the Rayleigh distribution for small SNR (i.e. $F/\sigma = 0$) and approaches a Gaussian distribution with mean F and variance σ^2 for large SNR [Schwartz]. Hence, for large SNR, the conditional probability of missed fault detection ($P_{01} = P_{MD}$) is approximated:

$$P_{MD} = P_{01} = \int_{-T_r}^{T_r} p(r \mid E_1)\, \partial r = \frac{1}{2}\,\mathrm{erf}\left(\frac{T_r - F}{\sigma\sqrt{2}}\right) - \frac{1}{2}\,\mathrm{erf}\left(\frac{-T_r - F}{\sigma\sqrt{2}}\right) = 1 - P_{11}$$

(Equation 4.35)

The conditional probability of fault isolation (P_I) is also difficult to solve. Again, the probability of correctly isolating any of the fault signatures ($\underline{f}_1$, $\underline{f}_2$, and $\underline{f}_3$) or their inverses is equal for all six cases and each case is equally likely (i.e. 1/6). We shall restrict the analysis to only one of the six possible cases: specifically, a positive fault on controller one ($\underline{f}_1$) where $f_1 = F$ and $f_2 = 0$. The marginal density function for the phase is found by averaging the joint density function over all possible radii: [Schwartz]

$$p(\theta \mid \underline{f}_1) = \int_0^\infty p(r, \theta \mid \underline{f}_1)\, \partial r = \frac{1}{2\pi} \exp\left(-\frac{F^2}{2\sigma^2}\right) + \frac{F\cos\theta}{2\sigma\sqrt{2\pi}} \exp\left(-\frac{F^2 \sin^2\theta}{2\sigma^2}\right) \left[1 + \operatorname{erf}\left(\frac{F\cos\theta}{\sigma\sqrt{2}}\right)\right]$$

$$p(\theta \mid \underline{f}_1) \cong \frac{F}{\sigma\sqrt{2\pi}} \exp\left(-\frac{F^2\theta^2}{2\sigma^2}\right) \quad \text{for large SNR and small angle } \theta$$

(Equation 4.36)

The marginal density of the phase is depicted in Figure 4.24 by Peebles. The curve is symmetrical about the assumed zero phase angle of the fault signature. For small SNR, the distribution reduces to a uniform probability of $1/2\pi$ as found earlier. For large SNR, the curve peaks markedly about the assumed phase angle and approaches an impulse function. Thus, the probability of fault isolation approaches certainty as the SNR increases. For large SNR and small angle θ, Schwartz found that the phase density can be approximated by a Gaussian distribution in radians of zero mean and a standard deviation equal to the SNR inverse of σ/F (Equation 4.36). [Schwartz] In this case, the conditional probability of fault isolation:

$$P_I = \int_{-\pi/6}^{\pi/6} p(\theta \mid \underline{f}_1)\, \partial\theta = \operatorname{erf}\left(\frac{\pi F}{6\sigma\sqrt{2}}\right)$$

(Equation 4.37)

For example, the probability of fault isolation is approximately 99.75% for a SNR of 5.77.

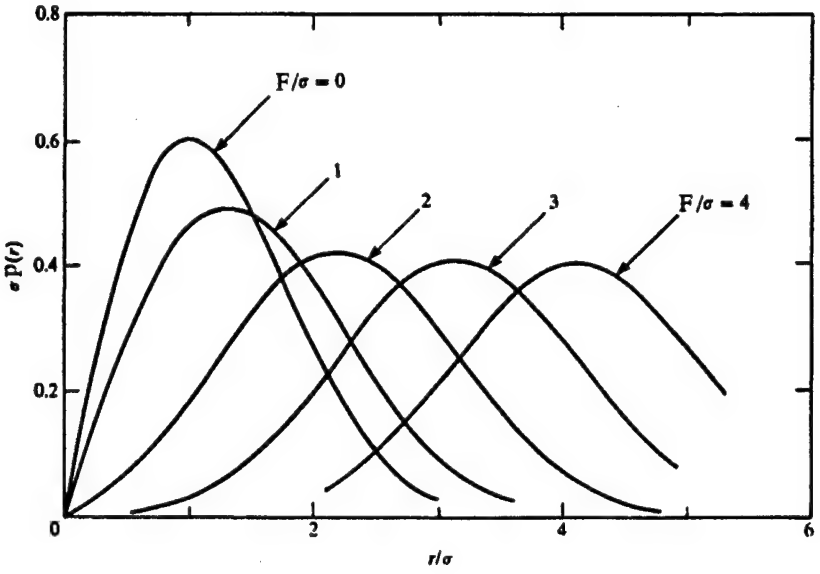


Figure 4.23

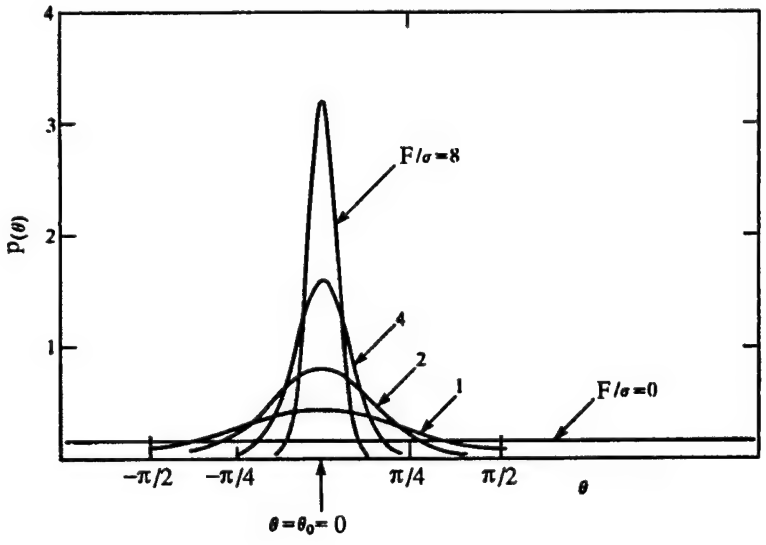


Figure 4.24

An average cost function or risk ($\mathfrak{R}$) equivalent to the probability of detection error (P_{Error}) is minimized with the likelihood ratio test (LRT). The likelihood ratio, denoted by $\Lambda(r)$, is determined directly from the ratio of the envelope's marginal densities under either event.

$$\Lambda(p_1,p_2) = \frac{p(p_1,p_2|\,E_1)}{p(p_1,p_2|\,E_0)} = \exp\left(\frac{1}{2\sigma^2}\left[(p_1^2 + p_2^2) - (p_1 - f_1)^2 - (p_2 - f_2)^2\right]\right)$$

(Equation 4.38)

However, the fault vector $\underline{f}$ of event E_1 is unknown a priori. The maximum likelihood (ML) estimate of the fault vector components f_1 and f_2 are those values which maximize the likelihood ratio. The above Equation 4.38 implies that the fault vector estimate of $\underline{f} = \underline{p}$ where $f_1 = p_1$ and $f_2 = p_2$ provides the maximum or worst-case likelihood ratio corresponding to our ignorance of the fault vector. [Walker, Whalen] Yet, we still wish to include our knowledge of the magnitude F of the fault vector in the analysis. Therefore, the squared magnitude $F^2 = 2/3\ f_{min}^2$ is substituted for $(f_1^2 + f_2^2)$ in the likelihood ratio and the ML estimate is utilized in all other instances:

$$\Lambda(p_1,p_2|\,\hat{f}_1=p_1,\,\hat{f}_2=p_2) = \exp\left(\frac{1}{2\sigma^2}\left[\,2p_1^2 + 2p_2^2 - F^2\right]\right)$$

(Equation 4.39)

As discussed in Section 4.3.2., the likelihood ratio is compared with the ratio of the priors $\eta = (P_0 - P_2 - P_3)/P_1 \approx P_0/P_1$ (Equation 4.15). The resultant test for our detection scheme compares the radius r to the derived threshold T_r and is thus generalized in order to account for a positive or negative fault in any controller.

$$|r| = \sqrt{p_1^2 + p_2^2} \quad \begin{matrix} \text{say } H_1 \\ > \\ < \\ \text{say } H_0 \end{matrix} \quad T_r = \sqrt{\sigma^2 \log \eta + \tfrac{1}{3} f_{min}^2}$$

(Equation 4.40)

Similarly, an average cost function or risk ($\mathfrak{R}$) equivalent to the probability of detection error must be determined and minimized with the likelihood ratio test (LRT) for each of the three possible fault signatures. The likelihood ratios, denoted $\Lambda_1(r)$, $\Lambda_2(r)$, and $\Lambda_3(r)$, are determined directly from the ratio of the envelope's marginal densities under event E_1 for the respective fault signature and event E_0. Here, the fault vector $\underline{f}$ of event E_1 is known a priori. The result is three tests comparing the absolute value of each fault signature's characteristic equation to a derived threshold T_I. They are generalized in order to account for a positive or negative fault in the controller.

Comparison Test for a Fault on Controller 1:

$$\Lambda_1(p_1,p_2|\, f_1 = F = \frac{2}{\sqrt{6}} f_{min},\, f_2 = 0) \;=\; \exp\Big(\frac{1}{2\sigma^2}\Big[\frac{4}{\sqrt{6}} p_1 f_{min} - F^2\Big]\Big)$$

$$\Big|\frac{2}{\sqrt{6}} p_1\Big| \;\underset{\text{say } H_0}{\overset{\text{say } H_1}{\gtrless}}\; T_I = \frac{\sigma^2}{f_{min}} \log\eta + \frac{1}{3} f_{min}$$

(Equations 4.41 - 4.42)

Comparison Test for a Fault on Controller 2:

$$\Lambda_2(p_1,p_2|\, f_1 = \frac{-1}{\sqrt{6}} f_{min},\, f_2 = \frac{1}{\sqrt{2}} f_{min}) \;=\; \exp\Big(\frac{1}{2\sigma^2}\Big[\frac{-2}{\sqrt{6}} p_1 f_{min} + \frac{2}{\sqrt{2}} p_2 f_{min} - F^2\Big]\Big)$$

$$\Big|\frac{-1}{\sqrt{6}} p_1 + \frac{1}{\sqrt{2}} p_2\Big| \;\underset{\text{say } H_0}{\overset{\text{say } H_1}{\gtrless}}\; T_I = \frac{\sigma^2}{f_{min}} \log\eta + \frac{1}{3} f_{min}$$

(Equations 4.43 - 4.44)

Comparison Test for a Fault on Controller 1:

$$\Lambda_3(p_1,p_2|\, f_1 = \frac{-1}{\sqrt{6}} f_{min},\, f_2 = \frac{-1}{\sqrt{2}} f_{min}) \;=\; \exp\Big(\frac{1}{2\sigma^2}\Big[\frac{-2}{\sqrt{6}} p_1 f_{min} + \frac{-2}{\sqrt{2}} p_2 f_{min} - F^2\Big]\Big)$$

$$\Big|\frac{-1}{\sqrt{6}} p_1 + \frac{-1}{\sqrt{2}} p_2\Big| \;\underset{\text{say } H_0}{\overset{\text{say } H_1}{\gtrless}}\; T_I = \frac{\sigma^2}{f_{min}} \log\eta + \frac{1}{3} f_{min}$$

(Equations 4.45 - 4.46)

A second method for fault detection can be formulated from the comparison tests for the individual fault signatures. With this additional knowledge of the fault signatures, the maximum likelihood (ML) estimate of the actual fault incurred is the average of the six possible cases: the three fault signatures and their respective inverses. However, the average of the six cases is zero due to the symmetry of the fault signatures. Thus, we shall take the average of the three generalized comparison tests above. This corresponds to the worst-case scenario of not knowing which of the three equally likely fault signatures has occurred. Yet, this still includes more information than the first method where we only knew the magnitude F of the fault vector. The resultant test is determined by first squaring both sides of the three generalized comparison tests and subsequently averaging the comparators on the left side of the equations:

$$\frac{2}{3}p_1^2 \underset{\text{say } H_0}{\overset{\text{say } H_1}{\gtrless}} T_I^2$$

$$\frac{1}{6}p_1^2 + \frac{1}{\sqrt{3}}p_1p_2 + \frac{1}{2}p_2^2 \underset{\text{say } H_0}{\overset{\text{say } H_1}{\gtrless}} T_I^2$$

$$\frac{1}{6}p_1^2 + \frac{-1}{\sqrt{3}}p_1p_2 + \frac{1}{2}p_2^2 \underset{\text{say } H_0}{\overset{\text{say } H_1}{\gtrless}} T_I^2$$

Averaging yields

$$|r| = \sqrt{p_1^2 + p_2^2} \underset{\text{say } H_0}{\overset{\text{say } H_1}{\gtrless}} T_r = \sqrt{3\,T_I^2} = \sqrt{\left(6\frac{\sigma^4}{f_{min}^2} + 2\sigma^2\right)\log\eta + \frac{1}{3}f_{min}^2}$$

(Equation 4.47)

where

$$|r| = \sqrt{\frac{2}{3}p_1^2 + \left(\frac{1}{6}p_1^2 + \frac{1}{\sqrt{3}}p_1p_2 + \frac{1}{2}p_2^2\right) + \left(\frac{1}{6}p_1^2 + \frac{-1}{\sqrt{3}}p_1p_2 + \frac{1}{2}p_2^2\right)} = \sqrt{p_1^2 + p_2^2}$$

A comparison of the two methods of fault detection is illustrated in Figures 4.25 and 4.26. Both methods compare the radius r of the parity vector to a derived threshold T_r. This optimal threshold is the essence and embodiment of each method and is the only true distinction between the two. Yet, one can observe a close resemblance between the two thresholds in Equations 4.40 and 4.47. The difference is that the coefficient of the first term (log η) is approximately twice as large for the second method as it is in the first method, while the second term remains the same. This causes the logarithmic effect of the ratio of priors (η) to be increased for the second method. The thresholds are equivalent for the two methods when the probability of any fault occurring is equal to the probability of normal operation ($p(E_0) = 1 - p(E_0) = 50\%, \eta = 1$). The threshold for the second method is initially greater than for the first at the beginning of the mission (large η) but has a faster descent to zero later in the mission (small η) when the probability of any fault occurring dominates the event space.

The resultant test is a more optimal detection scheme across the life of the mission. In this example, the probability of missed detection ($P_{MD} = P_{01}$) is found to dominate the probability of detection error. The probability of error is slightly greater for the second method initially due to a larger threshold, but becomes much smaller as the probability of any fault occurring becomes dominant and the threshold is more dramatically reduced. The probability of false alarms ($P_{FA} = P_{10}$) and of a dual or triple hidden fault ($p(E_2)$ and $p(E_3)$) are found to be relatively insignificant in this exercise. The optimality of the second method assumes a longer mission time where the control system goes through a number of successive stages of reduced operation. For very small mission times, the first method is a more optimal fault detection scheme. However, a triple redundant control structure would be inappropriate for short mission times.

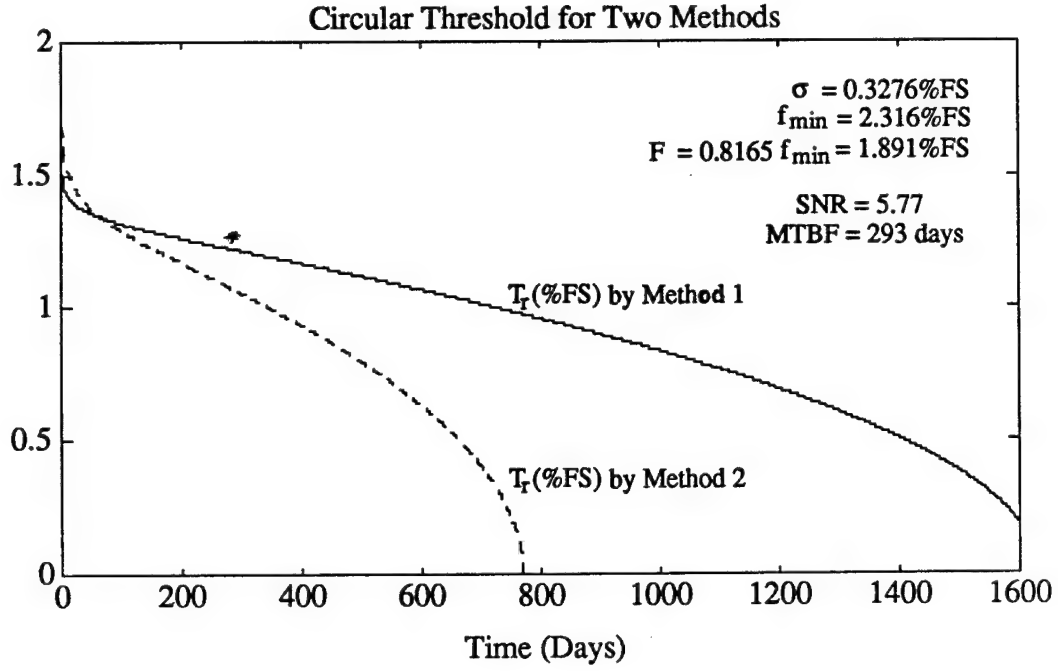


Figure 4.25

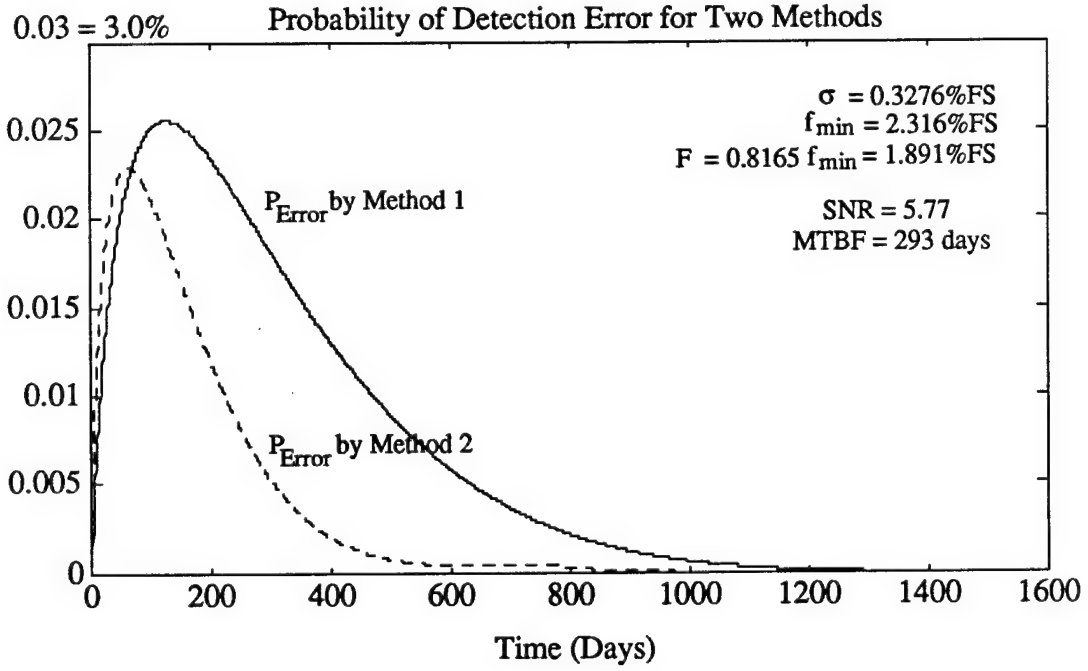


Figure 4.26

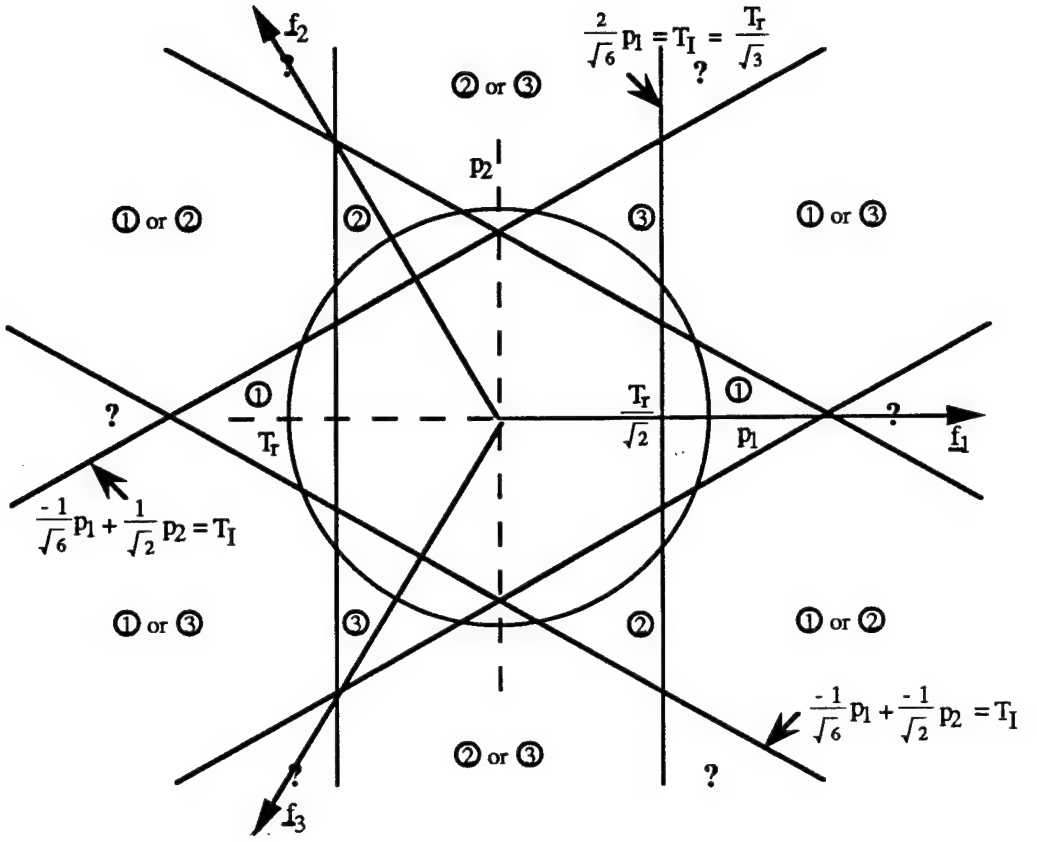
4.4.3. Triplex Fault Isolation and Reconfiguration

Upon fault detection within the control structure, diagnostic schemes must be initiated to isolate the failed structure(s), locate and report the faulty module(s), and reconfigure the system to provide continuous valid control. The balanced nature and symmetry of the TRS allows efficient fault detection and isolation for the controllers with the two-dimensional parity space. Each controller has a distinctive fault signature in this parity space. The collection of generalized comparison tests for these individual fault signatures (Equations 4.42, 4.44, and 4.46) can be used in a straightforward manner for a fault isolation scheme due to the uniform detectability of the fault signatures. The three generalized comparison tests section the parity space as depicted in Figure 4.27. Several sections overlap and therefore represent conflicting decisions between events. Conflict resolution is achieved by associating the faulty controller with the largest comparator C_i (Equation 4.48): [Gai]

$$\max\left\{C_1 = \left|\frac{2}{\sqrt{6}}p_1\right|;\ C_2 = \left|\frac{-1}{\sqrt{6}}p_1 + \frac{1}{\sqrt{2}}p_2\right|;\ C_3 = \left|\frac{-1}{\sqrt{6}}p_1 + \frac{-1}{\sqrt{2}}p_2\right|\right\} = C_i \Rightarrow \text{Fault on Controller i}$$

(Equation 4.48)

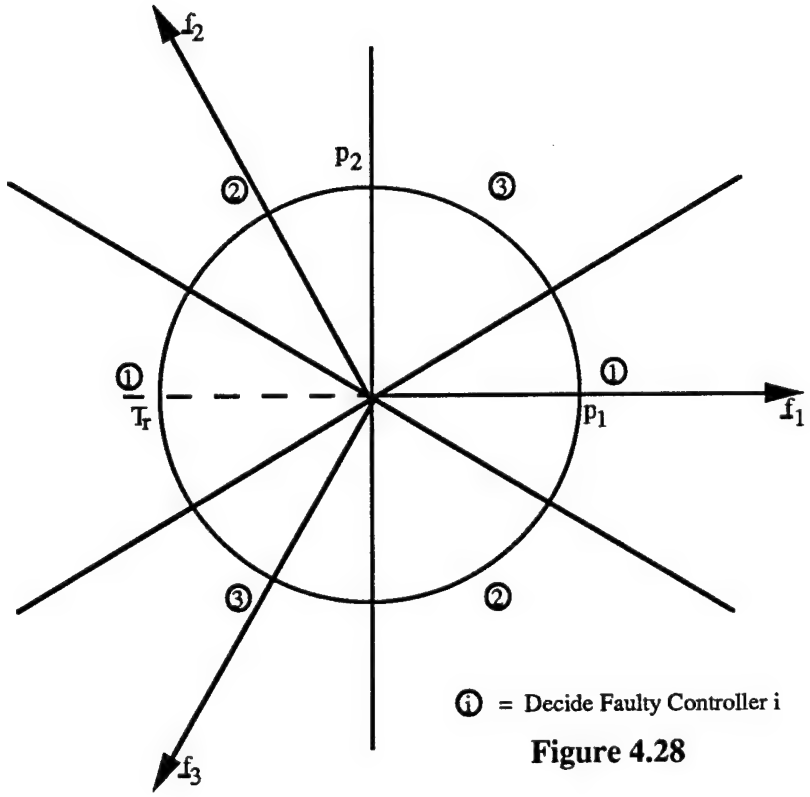
The resultant isolation scheme sections the parity space into six equal pie sections centered about the fault signatures and their inverses (Figure 4.28). It is assumed that fault isolation is only initiated upon detection of a fault. Thus, the central hexagon which represents the threshold for fault detection (Figure 4.27) is reduced to a point at the origin for the fault isolation scheme. This is equivalent to setting the threshold T_I for the comparison tests to zero. The conditional probability of fault isolation (P_I) for this decision area is derived above (Equation 4.37) and is conditioned upon fault detection.



① = Decide Faulty Controller i

? = ① or ② or ③

Figure 4.27



① = Decide Faulty Controller i

Figure 4.28

The conditional probability of fault isolation for dual faults must also be addressed. Assuming a uniform fault distribution where the fault vector has equal chances of occurring in any of the six pie sections of Figure 4.28, the conditional probability of dual fault isolation is easily determined to be two-thirds of the total possible decision area (P_{I2} = 66.6%). This allows correct isolation of the fault to either one of the two faulty controllers, while the other is reconfigured with the valid controller to the DDRS. Detection of the second fault would have to be accomplished at this secondary stage with the difference test. This is further analyzed below.

Similar to the hidden faults of the above detection scheme, there are dual faults which cause improper fault isolation for the isolation scheme. Incorrect isolation occurs with respect to a common bias fault: a dual fault where a fault of approximately equal amplitude occurs on two controllers (see Section 4.3.1, Figure 4.3). The combination of any two fault signatures of equal magnitude in the parity equation (Equation 4.26, 4.27) produces a fault vector equivalent to the inverse of the third fault signature. Our analysis of the DDRS suggested that the probability of a common dual fault on its two controllers is T/FS where T is the threshold of the difference test and FS is the fullscale for the parameter. There are three such possible pairings for the TRS (i.e. 12, 23, and 13) and each pairing has equal probability. Thus, we shall analyze only one pairing of a common bias fault on controllers two and three which produces a fault vector in the direction of $\pm\underline{f}_1$ (Figure 4.29). The shaded portion of Figure 4.29 represents the decision area of proper fault isolation (A_I) for the dual fault. For small thresholds T, this decision area is very small and the conditional probability of common bias fault isolation is approximated by the complement of the conditional probability of fault isolation ($P_{2B} = 1 - P_{I,}$ Equation 4.49). This is a worst-case approximation as the effects of the Gaussian error are not included. Note that hidden dual faults are also common bias faults.

Probability of a Common Bias Fault in TRS (given that a common bias has occurred)

$$\text{WOLOG, } f_1 = 0 \text{ and } |f_2 - f_3| \le T$$

$$\text{Thus, } p_1 = \frac{-1}{\sqrt{6}}(f_2 + f_3) \text{ and } p_2 = \frac{1}{\sqrt{2}}(f_2 - f_3)$$

$$\Pr\{ \text{Common Bias Isolation} \mid \text{TRS Common Bias \& Fault Detected} \} = P_{2B} =$$

$$\left(1 - \frac{A_I/FS^2}{T/FS}\right)(1 - P_I) = \left(1 - \frac{3T}{FS}\right)(1 - P_I)$$

$$\cong (1 - P_I) \quad \text{for small threshold T} \qquad \text{(Equation 4.49)}$$

$$A_I = \frac{1}{2} 3T\sqrt{2} \frac{T}{\sqrt{2}} \times 2 = 3T^2$$

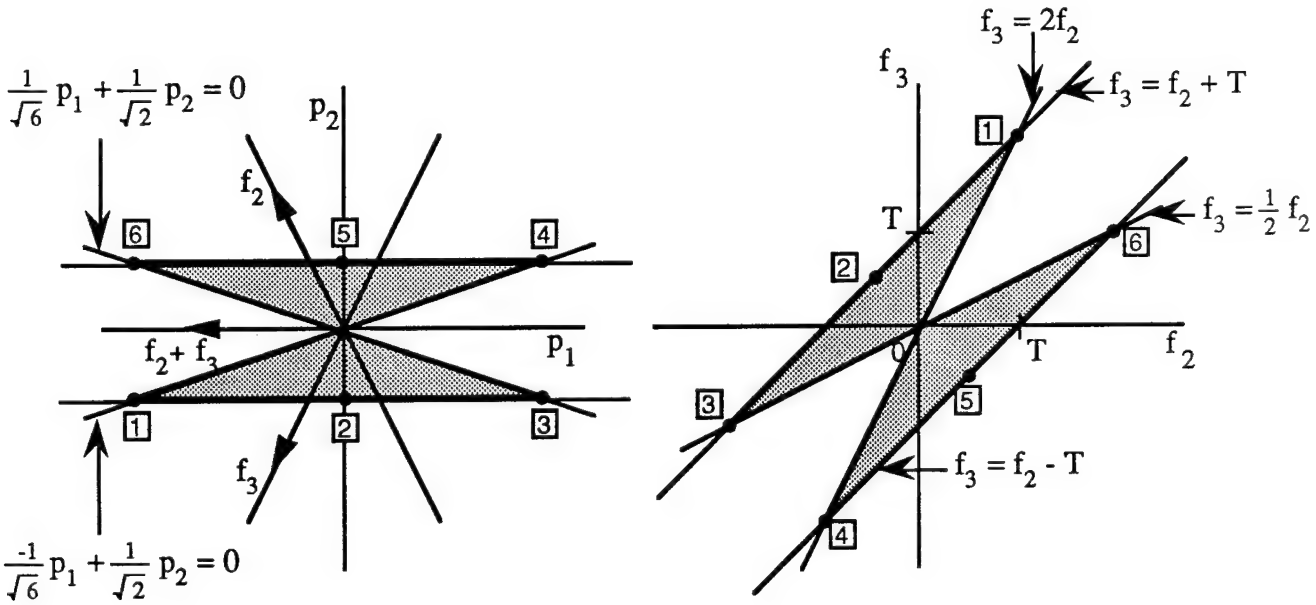


Figure 4.29 Common Bias Fault Represented in Parity and Fault Space

Reconfiguration consists of: 1) removing the faulty controller from the output estimation scheme (i.e. averaging) yet still including it as a voter in the FDI scheme of the TRS, and 2) immediately performing FDI as per the DDRS upon the two remaining valid control structures. The faulty controller is simply returned to valid status upon a successful comparison test for the TRS. This reconfiguration scheme allows recovery from false alarms and transient faults and maintains the independence between successive comparison tests of the TRS over the mission. However, upon reconfiguration to the DDRS, we are left with only one parity equation (i.e. the difference test) and the parity space shrinks down into a one-dimensional line in which direction is meaningless. Hence, a dual fault can only be detected, not isolated, efficiently by the DDRS (Section 4.3). Subsequent decisions must be based on further analysis of the individual controllers (simplex FDI, Section 4.2). Figure 4.30 depicts the decision tree associated with our FDI scheme for three levels of redundancy where correct decisions are denoted with a check mark. The probability of each possible system state and of the total system error can be directly determined from the decision tree (Equations 4.50 - 4.59). (Note: system shutdown is not considered as a possible system state in this exercise!)

System States for the TRS

1: Triple Structure, All Working
2: Triple Structure, Two Working
3: Triple Structure, One Working
4: Triple Structure, None Working
5: Dual Structure, Both Working
6: Dual Structure, One Working
7: Dual Structure, None Working
8: Single Structure, Working
9: Single Structure, Not Working

Probability of System Error for the TRS

$$P_{Error} = P_{S2} + P_{S3} + P_{S4} + P_{S6} + P_{S7} + P_{S9} + R_S^3 P_{10}^T + 3 Q_S R_S^2 P_{11}^T P_I P_{10}^D + 3 R_S Q_S^2 P_{11}^T (1 - P_I) P_{11}^D \frac{1}{2}$$

$$= Q_S^3 + 2 R_S Q_S^2 \quad \text{for the optimal fault detection and isolation scheme} \quad \text{(Equation 4.50)}$$

Probability of Each Possible System State for the TRS

$$P_{S1} = R_S^3 P_{00}^T;\ P_{S2} = 3 Q_S R_S^2 P_{01}^T;\ P_{S3} = 3 R_S Q_S^2 (P_{01}^T + (\frac{9 T_r^2}{8 FS^2}) (P_{00}^T - P_{01}^T));$$

$$P_{S4} = Q_S^3 (P_{01}^T + (\frac{7\sqrt{3}\ T_r^3}{16\sqrt{2}\ FS^3}) (P_{00}^T - P_{01}^T));\ P_{S5} = (R_S^3 P_{10}^T + 3 Q_S R_S^2 P_{11}^T P_I) P_{00}^D;$$

$$P_{S6} = (3 Q_S R_S^2 P_{11}^T (1 - P_I) + 3 R_S Q_S^2 (P_{11}^T \frac{2}{3} + \frac{T}{FS} P_{11}^T (1 - P_I - \frac{2}{3}) + \frac{9 T_r^2}{8 FS^2} (P_{10}^T - P_{10}^T P_I - P_{11}^T \frac{2}{3}))) P_{01}^D;$$

$$P_{S7} = (3 R_S Q_S^2 (1 - \frac{T}{FS} - \frac{9 T_r^2}{8 FS^2}) P_{11}^T \frac{1}{3} + Q_S^3 P_{11}^T (1 - \frac{7\sqrt{3}\ T_r^3}{16\sqrt{2}\ FS^3} - \frac{T}{FS} P_I)) P_{01}^D$$

$$+ (3 R_S Q_S^2 (\frac{T}{FS} P_{11}^T + \frac{9 T_r^2}{8 FS^2} P_{10}^T) P_I + Q_S^3 (\frac{T}{FS} P_{11}^T P_I + \frac{7\sqrt{3}\ T_r^3}{16\sqrt{2}\ FS^3} P_{10}^T)) P_{00}^D;$$

$$P_{S8} = (R_S^3 P_{10}^T + 3 Q_S R_S^2 P_{11}^T P_I) P_{10}^D$$

$$+ (3 Q_S R_S^2 P_{11}^T (1 - P_I) + 3 R_S Q_S^2 (P_{11}^T \frac{2}{3} + \frac{T}{FS} P_{11}^T (1 - P_I - \frac{2}{3}) + \frac{9 T_r^2}{8 FS^2} (P_{10}^T - P_{10}^T P_I - P_{11}^T \frac{2}{3}))) P_{11}^D \frac{1}{2};$$

$$P_{S9} = (3 R_S Q_S^2 (1 - \frac{T}{FS} - \frac{9 T_r^2}{8 FS^2}) P_{11}^T \frac{1}{3} + Q_S^3 P_{11}^T (1 - \frac{7\sqrt{3}\ T_r^3}{16\sqrt{2}\ FS^3} - \frac{T}{FS} P_I)) P_{11}^D$$

$$+ (3 R_S Q_S^2 (\frac{T}{FS} P_{11}^T + \frac{9 T_r^2}{8 FS^2} P_{10}^T) P_I + Q_S^3 (\frac{T}{FS} P_{11}^T P_I + \frac{7\sqrt{3}\ T_r^3}{16\sqrt{2}\ FS^3} P_{10}^T)) P_{10}^D$$

$$+ (3 Q_S R_S^2 P_{11}^T (1 - P_I) + 3 R_S Q_S^2 (P_{11}^T \frac{2}{3} + \frac{T}{FS} P_{11}^T (1 - P_I - \frac{2}{3}) + \frac{9 T_r^2}{8 FS^2} (P_{10}^T - P_{10}^T P_I - P_{11}^T \frac{2}{3}))) P_{11}^D \frac{1}{2}$$

Equations 4.51 - 4.59

where superscript T and D represent TRS and DDRS conditional probabilities, respectively.

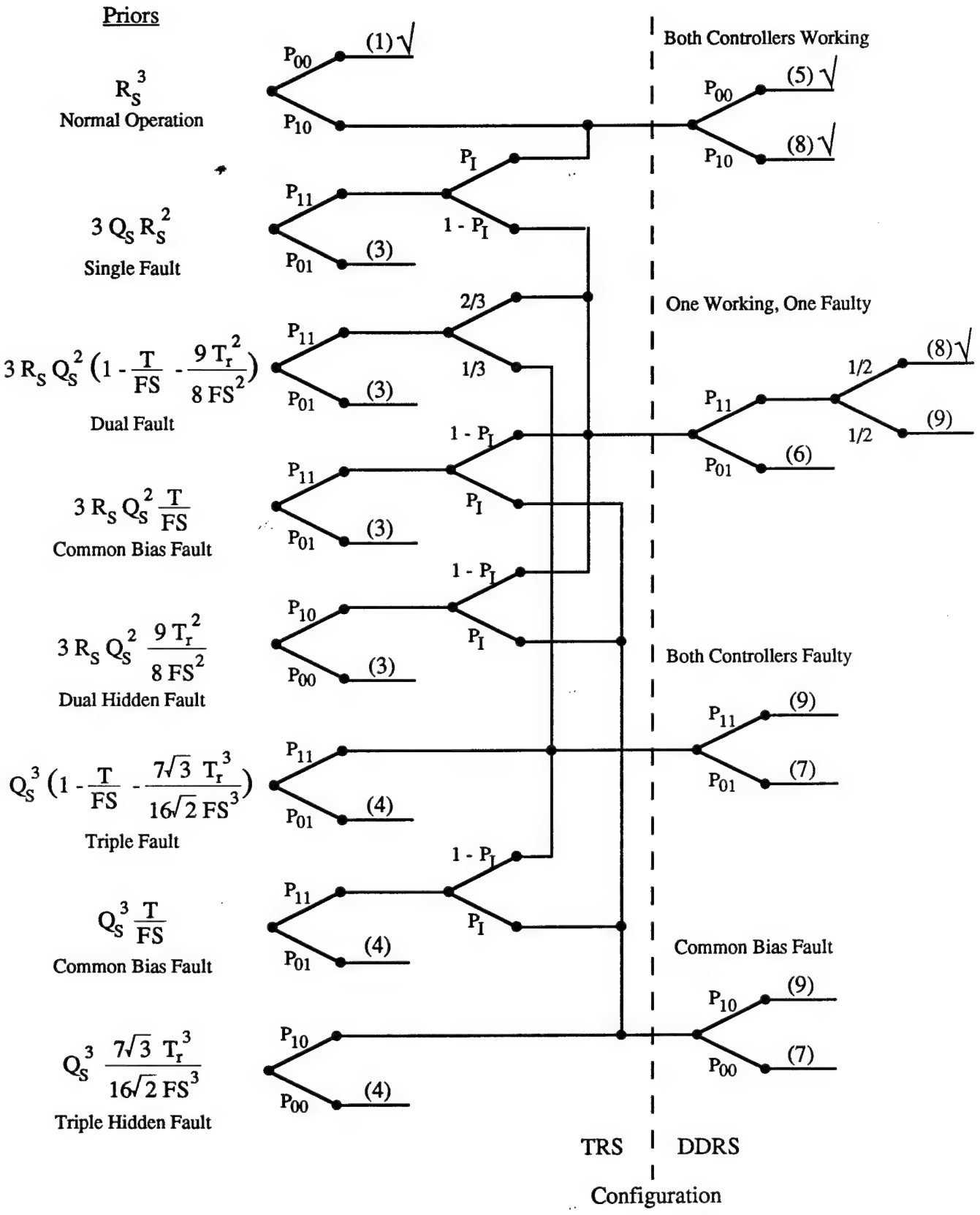


Figure 4.30 Decision Tree for FDI Scheme with Triple Redundancy

4.5. Unrecoverable Reconfiguration

A second method of reconfiguration for redundant structures upon fault detection and isolation is to simply ignore the faulty controller in all future operations. This method places a higher cost on structure performance under fault conditions than upon performance at a reduced level of redundancy. However, this static reconfiguration scheme does not allow for recovery from false alarms or transient faults. Further, the probability of false alarm over consecutive samples becomes a very important statistic and is found to quickly increase with the number of consecutive samples (k). This dramatic increase is due to the memory-less or independent nature of the single sample tests presented above for the FDI scheme. [Walker]

$$\Pr\{\text{Any False Alarm during k Consecutive Samples}\} = 1 - (1 - P_{FA})^{k} \qquad \text{(Equation 4.60)}$$

An example of this sequential decision error is presented in Figure 4.31 where P_{FA} = 0.27% (as determined for our example of a fault detection scheme for the DDRS based on the Neyman-Pearson criterion, Section 4.3.3). A small sample frequency relative to the MTBF of the controllers (e.g. 1 Hz.) would yield potentially disastrous results.

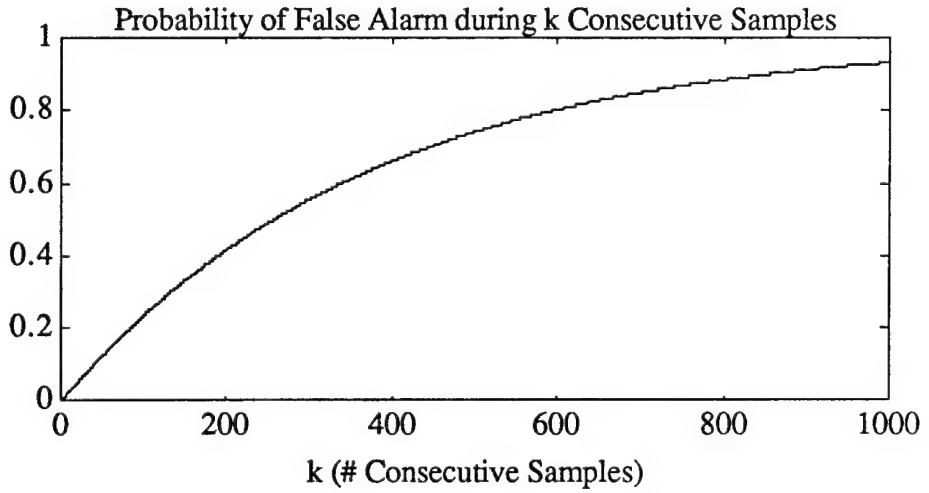


Figure 4.31

4.6. Conclusions

In contrast with current fault-tolerant control schemes, the dual-difference redundant structure (DDRS) and triple redundant structure (TRS) provide real-time fault detection and error accountability for sensor systems in an untended manufacturing environment without the use of a process model. Also, these active redundancy schemes are one step beyond passive schemes (e.g. TMR or NMR) towards complete fault coverage in that fault occurrences are detected and not merely screened. The control structures provide fault-tolerant control (i.e. fault detection, isolation, and reconfiguration) to the extent of their capabilities. Reconfiguration consists of a graceful and recoverable reorganization of the system to a structure of lesser redundancy and reduced performance. Hence, each redundant control structure is a subset of all structures of greater redundancy. For example, the triple redundant structure provides both efficient fault detection and isolation with a rather practical FDI scheme. Upon fault detection, the TRS is reconfigured to the DDRS with the two remaining valid controllers. In this manner, fault-tolerant control is achieved.

The fault detection and isolation (FDI) scheme assumes a classical, M-ary hypothesis test with a fixed, singular data sample. Thus, there are M possible alternatives or event-hypothesis pairings each time a decision must be made. With any decision-making process comes the possibility of decision errors; in this case, there is an inherent give-and-take between the two decision errors of false alarms and missed detections. With any FDI scheme, it is found that the probability of these decision errors is inversely proportional to the failure signal-to-noise ratio (SNR). This analysis is concerned with the worst-case fault magnitude of f_{min} which is the smallest fault (and, thus, the hardest to detect) of accountable cost for the current application. It is further generalized to account for both positive and negative faults. A second concern of decision error is the possible missed detection of certain multiple faults which are hidden from the FDI scheme. For

example, the difference test is insensitive to a dual fault where a fault of approximately equal amplitude occurs on both controllers. This analysis assumes a uniform fault distribution across the space of all possible faults and found the effect of multiple faults on the probability of decision error to be negligible. The resultant set of system states and their associated probabilities is determined from a decision tree for each redundant structure based on its FDI and reconfiguration schemes.

Several fault detection and isolation schemes are examined for each redundant structure. The FDI scheme can be optimized by using a generalized likelihood ratio test (GLRT) which is based on a degenerated Bayes criterion. This analysis utilizes the special cost assignment where correct decisions incur no penalty and incorrect decisions incur the same penalty. With this cost assignment, risk is equivalent to the probability of decision error. The likelihood ratio is determined directly from the ratio of the marginal or conditional densities of the parameter or parity vector under either event. Another possible FDI scheme is based upon the classical Neyman-Pearson criterion of radar detection theory. Here, the conditional probability of false alarms P_{FA} is constrained to remain less than some arbitrarily small value α, known as the level or significance level of the test, and then the conditional probability of fault detection P_D is maximized to some value $(1-\beta)$, known as the power of the test. The resultant test for either FDI scheme compares a significant statistic (e.g. the radius or absolute difference) to a derived threshold and is thus generalized in order to account for a fault in any controller. This threshold is held constant by the Neyman-Pearson criterion and is completely defined upon choosing the level of the test (α). For the Bayes criterion, the threshold is varied according to the prior event probabilities of the control structure in order to minimize the probability of decision error. For example, the threshold is originally made quite large compared to the fault magnitude while the probability of normal operation is high and is subsequently pulled closer to the origin as the probability of a structure fault becomes predominant.

In the next chapter, we analyze all relevant a priori uncertainty or entropy within the control system. The minimized Gaussian error function and the maximized exponential reliability function provide a complete concept of all a priori knowledge of the control structure. The marginal or conditional probabilities of the FDI schemes describe the performance statistics associated with the redundant structure. The resultant set of system states and their associated probabilities, as illustrated by the decision tree, represents all a priori uncertainty in the control system. Information theory defines entropy as a logarithmic measure of the randomness or 'choice' involved in an event or the prior uncertainty of the outcome of an experiment. This metric of uncertainty allows for comparisons of the effective system performance for different redundant structures.

Chapter 5: Entropy Analysis of Redundant Structures

The concept of entropy has a rich history that defies disciplinary boundaries in its application. The word "entropy" as a scientific concept was first used in thermodynamics by Clausius (1850). Its probabilistic interpretation in the context of statistical mechanics is attributed to Boltzman (1877). However, the explicit relationship between entropy and probability (Equation 5.1) was recorded several years later by Planck (1906). This thesis draws heavily from Shannon's celebrated paper (1948) on information theory where entropy is used as a measure of information (or, more to the point, missing information). Basic to the concept of information is the notion of uncertainty; the more uncertain we are about the outcome of an event, the greater will be the amount of information associated with the outcome. If we can predict in advance the outcome of an experiment, then no information has been conveyed by the experiment. Jaynes (1957) reexamined the method of maximum entropy (MEM) and applied it to a variety of problems involving the determination of unknown parameters from incomplete data. Other fields of research have also delved into the application of entropy. Weaver wrote:

> Dr. Shannon's work roots back ... to Boltzmann's observation, in some of his work on statistical physics (1894), that entropy is related to "missing information," inasmuch as it is related to the number of alternatives which remain possible to a physical system after all the macroscopically observable information concerning it has been recorded. Szilard (1925) extended this idea to a general discussion of information in physics and von Neumann (1932) treated information in quantum mechanics and particle physics. Weiner has been ... concerned with biological application (central nervous system, etc.). [Shannon]

The most famous application is the Second Law of Thermodynamics: the entropy of a system (e.g. the universe or a control structure) will always increase over time. An optimal structure or system design with respect to entropy would be one which originates with a minimal entropy from all perspectives and degrades at a minimal pace. This widespread

application of entropy attests to its fundamental nature and allows for linkage into a more comprehensive system representation of uncertainty by incorporation of other system entropies: the process and its disturbances [Papoulis], the control scheme [Weidemann, Weiner] and planning procedures [Valavanis], reasoning and other information processing algorithms [Stephanou], etc.

5.1. Measure of Uncertainty in the A Priori Knowledge

Our goal, thus far, has been the definition of all a priori knowledge associated with redundant structure performance. The reliability analysis defines how long the structure will operate without failure; while the error analysis defines how accurate the structure will operate given that no failure has occurred. Due to the inherent uncertainty in this knowledge, conditional error is characterized by a Gaussian density function and reliability by an exponential distribution. The marginal or conditional probabilities of the FDI schemes describe the performance statistics associated with the redundant structure. The resultant set of system states and their associated probabilities, as illustrated by the decision tree, represents all a priori uncertainty in the control system. Information theory defines entropy ($\mathfrak{H}$) as a measure of information, choice, and uncertainty. [Shannon] Entropy is a logarithmic measure of the randomness or 'choice' involved in an event or the prior uncertainty of the outcome of an experiment. It can be formulated from the probabilities of an exhaustive set of n possible events or experiments (discrete case) or from the pdf of a continuous distribution (continuous case):

$$\mathfrak{H} = -\sum_{i=1}^{n} p(X_i) \log p(X_i) = -\int_{-\infty}^{\infty} p(x) \log p(x)\, \partial x \qquad \text{(Equation 5.1)}$$

This formulation is particularly suited for representing the uncertainty inherent within discrete event sets for many reasons. Entropy increases monotonically with n and a

maximum entropy of (log n) is achieved when all n events are equally probable. This is intuitively the most uncertain situation. Any change towards equalization of the probabilities or uniformity in the density function causes a subsequent increase in the entropy. A minimum entropy of zero occurs when the outcome is known with certainty. Any change towards a dominant probability or a focusing of the density function allows for a subsequent decrease in the entropy. Otherwise, the entropy of discrete event sets is positive and is bounded by these extreme cases. An important property of entropy is that it is additive for independent experiments due to its logarithmic formulation. In conclusion, entropy is a measure of our a priori knowledge or, more appropriately, lack of knowledge (i.e. ignorance/uncertainty) in terms of our a priori probabilities. This metric of uncertainty allows for comparisons of the effective system performance for different redundant structures.

Uncertainty comparisons between discrete event sets can be easily made with an entropy analysis of their associated probability sets. Binary sets, consisting of an event and its complement, are the simplest case (n=2) and yet are the most important comparison size or dimension found within digital communication theory. The entropy of a binary set is maximized as the two events become equally probable ($p = 0.5$) and is minimized as one event becomes certain. These concepts of uniformity and polarity form the basis for comparisons between n-ary event sets. As mentioned above, any change or difference between two n-ary event sets towards equalization of the n discrete probabilities determines a corresponding increase in the entropy of the sets (i.e. in comparison, a trend towards uniformity in the probabilities indicates a trend towards greater entropy in the event sets). The fact that entropy increases monotonically with n allows for comparisons of event sets of different sizes. All things being equivalent, a discrete event set of larger size will have greater entropy due to the added complexity of additional states. Thus, comparisons of our uncertainty about different discrete event sets are facilitated by entropy.

The entropy of a continuous distribution is defined in an analogous manner to the entropy of discrete event sets (Equation 5.1). However, an important distinction exists between the two cases. In the discrete case, the chance variables are the events which are mutually exclusive and their union is the certain event ($p_1 + p_2 + ... p_n = 1$). Entropy is defined for a given partition of the event space into a set of n distinct events. The uncertainty or randomness of the events is, therefore, measured in an absolute way (i.e. relative to the n-ary partition and its associated n probabilities; irrespective of the event space) and, as seen in the preceding paragraph, this allows for direct numerical comparisons of the entropies of discrete event sets. Uncertainty comparisons can even be made between two independent event sets which have nothing to do with one another (e.g. apples and oranges). In the continuous case, the chance variable is a measurement whose value is relative to a coordinate system with an assumed standard or measurement scale. The entropy of a continuous distribution cannot be defined in an absolute fashion because the events do not form a partition ($n = \infty$) and are of an arbitrary size dependent on the coordinate system. Comparisons cannot be made between coordinate systems unless the transformation or relationship between their respective unit volumes/vectors is known. Uncertainty comparisons, therefore, can only be made between continuous distributions transformed into or originating from the same coordinate system. Transformation of a density function (Section 5.3) would assign a new entropy to the distribution relative to the new coordinate system.

In spite of this dependence on the coordinate system, the entropy concept is as important in the continuous case as in the discrete case. In fact, one conventional uncertainty comparison is the change or difference in the entropy of a specific variable's distribution (as opposed to uncertainty comparisons between multiple variables) as the system passes into some other state or is affected by some event. In addition, the entropies

of continuous distributions have most, but not all, of the properties of the discrete case. Other distinctions due to this arbitrary scale of reference are listed hereafter:

The entropy of a continuous distribution can take any value in $(-\infty, \infty)$. Zero entropy for a given measurement scale corresponds to a uniform density over a unit volume ($\mathcal{H} = \int\int\ldots\int 1 \log 1 \, dx_1 dx_2 \ldots dx_n = 0$) and any distribution of smaller volume will have a negative entropy.

If the density function is bandlimited to a finite volume α, maximum entropy of ($\log \alpha$) corresponds to a uniform density of $p(x) = 1/\alpha$ for all x:

$$\mathcal{H} = -\int_0^{\alpha} \frac{1}{\alpha} \log \frac{1}{\alpha} \, \partial x = -\log \frac{1}{\alpha} = \log \alpha$$

(Equation 5.2)

If the density function is limited to an average power, maximum entropy corresponds to a Gaussian density:

$$p(x) = \text{Gaussian}(0,\sigma) = \frac{1}{\sigma\sqrt{2\pi}} e^{-x^2/2\sigma^2} \quad \text{where} \quad \sigma^2 = \int p(x)\, x^2 \, \partial x$$

$$-\log p(x) = \log \sigma\sqrt{2\pi} + \frac{x^2}{2\sigma^2}$$

$$\mathcal{H}(x) = \log \sigma\sqrt{2\pi} \int p(x) \, \partial x + \frac{1}{2\sigma^2} \int p(x)\, x^2 \, \partial x$$

$$= \log \sigma\sqrt{2\pi} + \frac{1}{2} = \log \sigma\sqrt{2\pi e}$$

(Equation 5.3)

This direct relationship between entropy and variance implies that a minimum mean-square error (MSE) design for Gaussian random variables is always a minimum entropy design.

If the density function is limited to a half-line ($p(x) = 0$ for $x \leq 0$) and the first moment or mean is fixed at β, maximum entropy corresponds to an exponential density:

$$p(x) = \frac{1}{\beta} e^{-x/\beta} \quad \text{where } \beta = \int p(x)\, x\, \partial x$$

$$\mathcal{H}(x) = \log \beta \int p(x)\, \partial x + \frac{1}{\beta} \int p(x)\, x\, \partial x = \log e\beta$$

(Equation 5.4)

The entropy of the Gaussian conditional error function for an N redundant control structure is $\mathcal{H}(\varepsilon) = \log(\sigma\sqrt{2\pi e/N})$ by Equations 3.3 and 5.3. The entropy of redundant structures can be directly compared with respect to their scaling in %FS and it is observed that the entropy of the error distribution is reduced with the level of redundancy employed. The failure time density of the control structure is an exponential function (Equation 3.10) limited to a half-line due to the causal nature of the process and has a fixed mean which is estimated by MTBF. By Equation 5.4, the entropy of the failure time density is, therefore, $\mathcal{H}(f) = \log(e/\lambda) = \log(e * \text{MTBF})$ and is directly related to the structure's MTBF. Redundancy of the control structure provides an increase in the system MTBF and entropy.

Note that error and reliability are represented by distributions which maximize the entropy with respect to the given information. Jaynes found that Information Theory provides a constructive criterion (i.e. the maximum entropy method, MEM) for setting up probability distributions on the basis of partial knowledge. [Jaynes] Among all distributions which are concomitant with the available information, the selected density function is the one which is maximally vague or minimally prejudiced regarding the missing information. Jaynes further showed that the theory of MEM statistical inference is mathematically identical with the rules of calculation provided by statistical mechanics. Tribus demonstrated that all of the laws of classical thermodynamics can be defined from Shannon's entropy using the principle of maximum entropy. [Tribus]

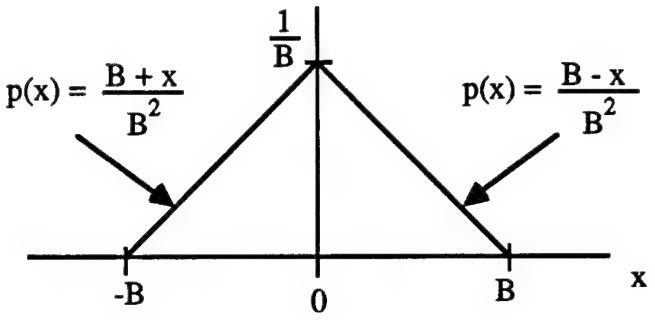


Figure 5.1 Triangular Probability Density Function

The entropy of a triangular probability density function (Figure 5.1) can also be derived. Averaging two independent random variables with uniform distributions of base width 2B results in a triangular density of base width 2B. [Peebles]

$$\mathcal{H}(x) = -\int_{-B}^{0}\left(\frac{B+x}{B^2}\right)\log\left(\frac{B+x}{B^2}\right)\partial x \; -\int_{0}^{B}\left(\frac{B-x}{B^2}\right)\log\left(\frac{B-x}{B^2}\right)\partial x$$

$$\mathcal{H}(x) = \frac{x^2}{4B^2} + \frac{x}{2B} - \left(\frac{x^2}{2B^2} + \frac{x}{B} + \frac{1}{2}\right)\log\left(\frac{B+x}{B^2}\right)\Big]_{-B}^{0}$$

$$+ \frac{-x^2}{4B^2} + \frac{x}{2B} - \left(\frac{-x^2}{2B^2} + \frac{x}{B} - \frac{1}{2}\right)\log\left(\frac{B-x}{B^2}\right)\Big]_{0}^{B}$$

$$\mathcal{H}(x) = \left[-\frac{1}{2}\log\left(\frac{1}{B}\right) - \frac{1}{4} + \frac{1}{2}\right] + \left[-\frac{1}{4} + \frac{1}{2} - \frac{1}{2}\log\left(\frac{1}{B}\right)\right]$$

$$= -\log\left(\frac{1}{B}\right) + \frac{1}{2} = \log(B\sqrt{e})$$

(Equation 5.5)

This distribution can be approximated by a Gaussian distribution with a standard deviation of $\sigma_{2F} = B/\sqrt{6}$ by Equation 3.6 and with an entropy of $\mathcal{H}(\varepsilon) = \log(B/\sqrt{\pi e/3}) \approx \log(B\sqrt{e})$ by Equation 5.3. The entropy of the triangular density is found to increase with the base width and is less than the entropy of a uniform density (Equation 5.2) of same base width ($\alpha = 2B$) by an amount of $\log(2/\sqrt{e}) = 0.2$.

5.1.1. Structure Certainty vs. Structure Performance

The entropy of the reliability distribution is interpreted as our uncertainty of the normal behavior or operation of the control structure over time (with respect to some unit of time). The greater the control structure's MTBF; the bigger the reliability distribution over time; and, therefore, the greater the entropy of the controller (Equations 5.4). In an uncertainty comparison with respect to a common time frame, we are more certain in the failure time of the controller with the smaller MTBF and reliability distribution. This is due to two factors of the smaller distribution with respect to the larger distribution: the quicker descent of its reliability over time (we quickly lose faith in its performance while our period of uncertainty in the other controller's performance is much longer) and the fact that its reliability approaches zero sooner (we become certain that a failure has occurred while we are still unsure of the other controller's performance). These results are determined from Equation 5.4 with respect to the failure time density function f(t) and its distribution (i.e. the unreliability Q(t)). The structure with greater MTBF has a failure function with greater spread and therefore greater entropy (Figure 5.2).

This representation of our uncertainty in a control structure's reliability betrays the intrinsic trust or confidence we place in a controller with a greater MTBF and reliability distribution. We assert that, "We are certain that the controller with a greater MTBF is more reliable over the mission time." The important distinction to be made is that the entropy of a control structure variable, as defined in Equation 5.1, is a measure of the uncertainty in the knowledge of that variable (as defined by its pdf) and not a measure of the chaos or discord caused by the variable to the structure. A control structure with lower entropy is not necessarily a better system; we could be highly certain that the structure is inoperative or in some other unwanted state. Care must be taken not to reduce uncertainty at a cost to performance of the control structure.

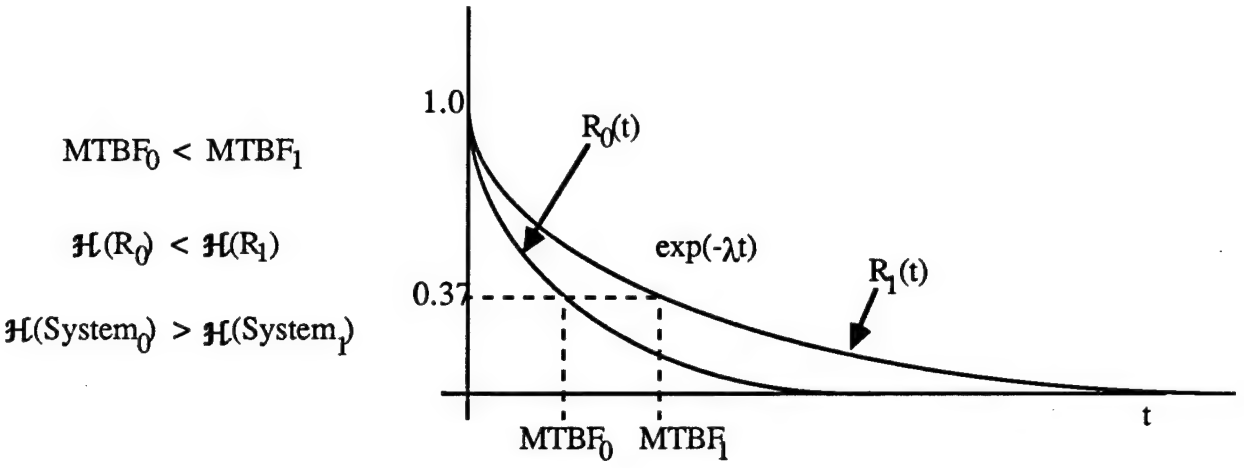


Figure 5.2 Entropy Comparison of the Reliability of Two Structures

Certainty in knowing the state of a system ≠ Certainty or Confidence in system performance

5.2. Effect of Transformations on Entropy

A special case of dependent event sets or distributions is when the dependence of the event sets can be expressed as a transformation or function of one event to the other. This transformation between event sets X and Y can be expressed by the equation $y = g(x)$ and, in this case, the entropies of the event sets can be compared with one another. Independent event sets cannot be represented with a transformation. If the transformation has a unique inverse $x = g^{-1}(y)$, then there exists a one-to-one correspondence between the domain and range of the function (here, the discrete events of X and Y) and, therefore, $p(Y = y_i) = p(X = x_i)$ for $i = 1...n$. For an invertible transformation, $\mathcal{H}(Y) = \mathcal{H}(X)$. If the transformation does not have a unique inverse, then there exists a solution y for more than one value of x. Thus, the event set X is of larger size than the event set Y and has greater entropy ($\mathcal{H}(Y) < \mathcal{H}(X)$) due to the added complexity of additional states. Here, the transformation $y = g(x)$ on the discrete event space X has resulted in a reduction in the entropy. Similar results follow from the continuous case: [Papoulis]

If the dependence between two continuous variables can be represented by the transformation $y = g(x)$, then

$$\mathcal{H}(y) \leq \mathcal{H}(x) + E\{\ln |g'(x)|\} \qquad \text{(Equation 5.6)}$$

with equality iff the transformation is invertible.

If the dependence between two continuous vectors can be represented by a set of n functions $y_i = g_i(x_1,..., x_n)$, then

$$\mathcal{H}(y_1,...,y_n) \leq \mathcal{H}(x_1,...,x_n) + E\{\ln |J(x_1,...,x_n)|\} \qquad \text{(Equation 5.7)}$$

with equality iff the transformation is invertible and where $J(x_1,...,x_n)$ is the Jacobian of the transformation.

If the dependence between two continuous vectors can be represented by a set of n linear transformations $y_i = g_i x_i = a_{i1}x_1 + \ldots + a_{in}x_n$, then

$$\mathcal{H}(y_1,...,y_n) = \mathcal{H}(x_1,...,x_n) + \ln |\Delta| \qquad \text{(Equation 5.8)}$$

where Δ denotes the determinant of transformation matrix G.

As an exercise, consider the linear transformation of rescaling the error budget of the control structure (Equation 2.1) from units of %FS to Volts for a fullscale value of 10 Volts. This can be represented as $y = x*10/100\% = x/10\%$. The derivative of the transformation $g'(x)$ and the determinant of the [1x1] transformation matrix G is 1/10. The probability density for the control structure error is defined as Gaussian and the entropy of this pdf is directly dependent on the standard deviation (Equation 5.3). For our example error budget, the standard deviation would be rescaled from 0.3276%FS to 0.03276 Volts by this linear transformation. The resulting entropy of the error density scaled in Volts is found to be less than the entropy of the same error density scaled in %FS (Equations 5.6, 5.8). This exercise shows the dependence of entropy upon the coordinate system in defining the uncertainty of a continuous density.

$$\mathcal{H}(y) = \log(0.3267\%FS\sqrt{2\pi e}) + \log(0.1) = \log(0.03267V\sqrt{2\pi e}) = 0.135$$

5.3. The Measure Function

A second formulation for the entropy of continuous distributions is suggested (Equation 5.9). Jaynes refers to the addition m(x) to the entropy formulation as a "measure function" which is proportional to the limiting density of the discrete or sampled points of the density function p(x). If the precision of the random variable or coordinate system is given as $\pm \Delta_x/2$, then the limiting density function is a uniform $1/\Delta_x$ about each point. Regardless, the measure function m(x) is introduced in Equation 5.9 in order to make the expression dimensionless under the logarithm and to remove the dependence upon coordinate system. Hence, the choice of measure function determines the position of zero on the entropy scale and is completely arbitrary. In particular, we might make $m(x) = \Delta_x = 1$ to retain Shannon's formulation (Equation 5.1) and thereby associate zero entropy with the standard unit of measurement for p(x). Proper choice of the measure function allows for comparisons between continuous distributions by placing them on the same entropy scale (i.e. with respect to m(x)). In addition, joint entropies can be formulated due to our understanding of the relative contributions from different variables upon system entropy. This understanding is not possible with Shannon's formulation of entropy. [Jaynes, Papoullis, Pugachev]

$$\mathcal{H} = -\int_{-\infty}^{\infty} p(x) \log \frac{p(x)}{m(x)} \, \partial x = -\int_{-\infty}^{\infty} p(x) \log p(x) \, \partial x - \log \Delta_x$$

(Equation 5.9)

Note that the equations for Shannon's entropy need only slight modification (i.e. subtracting $\log \Delta_x$ from its final form) to achieve Equation 5.9. We shall refer to Equation 5.9 as the entropy for continuous distributions in all further discussions.

The major change of this reformulation is that entropy is unaffected by rescaling of the coordinate system and invariant to invertible transformations by proper choice of the measure function m(x). First, we will consider rescaling of the coordinate system. Since both the density p(x) and measure m(x) functions are of the same coordinate system, both functions are transformed in the same fashion upon a change or rescaling of the variable x. These changes cancel each other out in the logarithm and therefore entropy is invariant to a change in variable. Second, Equations 5.6 - 5.8 describe the effect of a transformation upon Shannon's entropy of a continuous variable or vector. Application of the measure function is straightforward. For example, the entropy of the variable x upon invertible transformation g(x) to the variable y is redefined as:

$$\mathfrak{H}(y) = \mathfrak{H}(x) + E\{\log |g'(x)|\} + \log \frac{\Delta_x}{\Delta_y} = \mathfrak{H}(x) + E\{\log \frac{\Delta_x}{\Delta_y} |g'(x)|\}$$

(Equation 5.10)

If two continuous distributions are related by an invertible transformation, then uncertainty comparisons are possible with respect to the measure functions by Equation 5.10. The entropy of the random variable is unaffected by the invertible transformation $y = g(x)$ (i.e. $\mathfrak{H}(y) = \mathfrak{H}(x)$) by proper choice of the measure function Δ_y:

$$\Delta_y = \Delta_x * |g'(x)|$$

(Equation 5.11)

For scaling or linear transformations, this choice of the measure function Δ_y is equivalent to the transformation of the measure function Δ_x and is determined by:

$$\Delta_y = \text{the transformation of } \Delta_x = g(\Delta_x) = \Delta_x * |g'(x)| = \Delta_x * \text{gain}.$$

(Equation 5.11)

In this manner, all random variables associated by an invertible transformation contain exactly the same amount of information. Entropy is invariant to invertible transformation.

5.4. Conditional and Joint Entropy

Another special case of probability is when the event sets or distributions are conditioned upon one another. This dependence between event probabilities in a set is expressed by conditional probabilities $p(X_i|Y_j)$ and the probability of an event in set X is defined by the theorem of total probability (Equation 5.12). Similarly, dependence between the probabilities of continuous variables is expressed by a conditional probability density p(x|y). Independent event sets or variables can be represented with an equivalent conditional probability set or a uniform conditional probability density. Equation 5.13d defines the mean conditional entropy $\mathcal{H}(X|Y)$ of event set X with respect to event set Y as the average of the entropy of the conditional probability set weighted by the probability of getting that particular Y. Similarly, Equation 5.13c defines the mean conditional entropy of a variable x with respect to a variable y. This quantity measures how certain we are of X on the average when we know Y. Equation 5.14d and 5.14c define the joint entropy $\mathcal{H}(X,Y)$ of event sets or continuous variables X and Y as the sum of the entropy of Y and the mean conditional entropy of X with respect to Y, or vice versa. There are two important results from this exercise. First, the entropy of an event set or variable monotonically decreases as it is conditioned on other event sets or variables ($\mathcal{H}(X|Y) < \mathcal{H}(X)$). Our uncertainty over an event set or variable is reduced when we can base our decision on its relation to other event sets or variables. Independent event sets or variables cause no such reduction in entropy ($\mathcal{H}(X|Y) = \mathcal{H}(X)$). Second, the joint entropy of event sets or variables is reduced if they are conditioned on one another. This follows directly from the fact that independent events/variables cause no reduction in the conditional entropies of the events/variables. As stated above, the entropy of independent event sets or variables is merely the sum of the entropies of each component:

$$(\mathcal{H}(X,Y)_{dependent} = \mathcal{H}(Y) + \mathcal{H}(X|Y) \; < \; \mathcal{H}(X,Y)_{independent} = \mathcal{H}(Y) + \mathcal{H}(X)).$$

Therefore, the worst-case or maximum joint entropy can always be defined as the direct sum of the component entropies. In addition, the joint entropy function (Equation 5.14) possesses an additivity property which allows the partitioning of the overall uncertainty of several variables into the uncertainty of the first plus the uncertainty of the second remaining after knowledge of the first, etc. [Shannon]

Discrete Event Sets

$$p(X_i) = p(X_i|Y_1)p(Y_1) + p(X_i|Y_2)p(Y_2) + \ldots + p(X_i|Y_n)p(Y_n) \qquad \text{(Equation 5.12)}$$

$$\mathcal{H}(X|Y) = -\sum_j p(Y_j) \sum_i p(X_i|Y_j) \log p(X_i|Y_j) = \sum_j p(Y_j)\, \mathcal{H}(X|Y_j) < \mathcal{H}(X)$$

(Equation 5.13d)

$$\mathcal{H}(X,Y) = -\sum_{i,j} p(X_i,Y_j) \log p(X_i,Y_j) = \mathcal{H}(Y) + \mathcal{H}(X|Y) = \mathcal{H}(X) + \mathcal{H}(Y|X)$$

(Equation 5.14d)

Continuous Distributions

$$\mathcal{H}(X|Y) = -\int p(y) \int p(x|y) \log \frac{p(x|y)}{m(x)}\, \partial x\, \partial y = -\iint p(x,y) \log \frac{p(x,y)}{p(y)\, m(x)}\, \partial x\, \partial y < \mathcal{H}(X)$$

(Equation 5.13c)

$$\mathcal{H}(X,Y) = -\iint p(x,y) \log \frac{p(x,y)}{m(x)\, m(y)}\, \partial x\, \partial y = \mathcal{H}(Y) + \mathcal{H}(X|Y) = \mathcal{H}(X) + \mathcal{H}(Y|X)$$

(Equation 5.14c)

However, one cannot say anything in comparison of $\mathcal{H}(X)$ and $\mathcal{H}(Y)$ by merely knowing that they are conditioned on each other. Given high confidence in X, this does not mean we have high confidence in Y when it is conditioned on X (i.e. its dependence may be weak, its conditional probabilities approaching equivalence). The inherent difficulties of uncertainty comparisons between continuous variables holds for conditional variables (i.e. arbitrary scaling or coordinate systems). Therefore, a measure function is still required to properly formulate a joint entropy or make any uncertainty comparisons.

5.5. Mutual Information and the Information Rate

The mutual information I(x,y) between two random variables is defined as the measure of the amount of information given for one variable by observing the other. Equivalently, it is viewed as a measure of the reduction of uncertainty within one variable upon knowing the other. Mutual information can be represented in many equivalent forms:

$$I(x,y) = \mathcal{H}(X) - \mathcal{H}(X|Y) = \mathcal{H}(Y) - \mathcal{H}(Y|X) = \mathcal{H}(X) + \mathcal{H}(Y) - \mathcal{H}(X,Y)$$

(Equation 5.15)

$$I(x,y) = I(y,x) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} p(x,y) \log \frac{p(x,y)}{p(x)\,p(y)}\, \partial x\, \partial y \geq 0$$

(Equation 5.16)

Note that mutual information cannot be negative because $\mathcal{H}(X) \geq \mathcal{H}(X|Y)$ (Equation 5.13) and is zero for independent random variables because the uncertainty in one variable is unaffected by knowing the other ($\mathcal{H}(X|Y) = \mathcal{H}(X)$). [Pugachev]

Invertible transformations are a member of a special class of "information preserving transformations". [Weidemann] From Section 5.2, entropy is invariant to invertible transformations $y = g(x)$ such that:

$$I(X,Y) = \mathcal{H}(X) = \mathcal{H}(Y) \quad \text{and} \quad \mathcal{H}(X|Y) = \mathcal{H}(Y|X) = 0$$

For any other random variable z:

$$\begin{aligned}\mathcal{H}(X|Z) &= \mathcal{H}(X,Y,Z) - \mathcal{H}(Z) - \mathcal{H}(Y|X,Z) \\ &= \mathcal{H}(X,Y,Z) - \mathcal{H}(Z) - \mathcal{H}(X|Y,Z) = \mathcal{H}(Y|Z)\end{aligned}$$

Therefore: $I(X,Z) = \mathcal{H}(X) - \mathcal{H}(X|Y) = \mathcal{H}(Y) - \mathcal{H}(Y|X) = I(Y,Z)$

Consequently, invertible transformation of a random variable does not change the mutual information it may have with any other random variable. In practice, however, operations upon a random variable are accompanied by a loss of information due to noise or other interference.

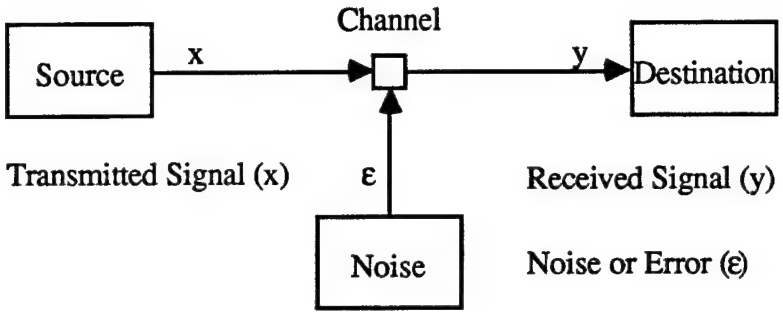


Figure 5.3 General Communication System

Shannon evaluated the performance of a general communication system in the presence of noise (Figure 5.3). In this context, a control structure can be considered the channel which attempts to communicate control needs to the process while contending with error or noise sources inherent within the signal transmission. These error sources are represented by the error budget of Chapter 2. Due to these errors, it is not possible to completely reconstruct the transmitted signal by any operation upon the received signal and information is lost. Shannon found methods of transmitting or encoding the source signal which are optimal in combating noise (detailed below). In this thesis, the source is fixed and minimization of the information lost is the only possible optimization of the system.

The rate of information transmission (R) across the channel is expressed as the mutual information between the transmitted and received signals (Equation 5.15, 5.16). The first defining expression, $\mathcal{H}(X) - \mathcal{H}(X|Y)$, can be interpreted as the amount of information sent less the uncertainty of what was sent; the second, $\mathcal{H}(Y) - \mathcal{H}(Y|X)$, measures the amount received less the part which is due to noise. The ideal, noiseless case is presented above as invertible transformation. No information is lost by such "information preserving transformations" and transmission is simply the entropy of the source ($R = \mathcal{H}(X)$). The worst case of noise or interference occurs when the transmitted and received signals are independent. Here, the rate of information transmission is zero ($R = 0$). The optimal rate of transmission for a system is one which maximizes the mutual information between the source and output of the channel.

The capacity (C) of a noisy communication system is defined as the optimal or maximum possible rate of transmission over the channel. A communication system reaches capacity when its information source is "matched" to its channel. Optimization of the rate of transmission consists of minimizing the lost information due to noise while maximizing the information contained within the source:

$$\max I(x,y) = \max (\mathcal{H}(X) - \mathcal{H}(X|Y)) \Rightarrow \max \mathcal{H}(X) \text{ and } \min \mathcal{H}(X|Y) \quad \text{(Equation 5.17)}$$

Alternatively, optimization of the rate of transmission consists of minimizing the interference while maximizing the information contained within the received signal:

$$\max I(x,y) = \max(\mathcal{H}(Y) - \mathcal{H}(Y|X)) = \max(\mathcal{H}(Y) - \mathcal{H}(\varepsilon)) \Rightarrow \max \mathcal{H}(Y) \text{ and } \min \mathcal{H}(\varepsilon) \quad \text{(Equation 5.18)}$$

In this thesis, the source is fixed and minimization of the interference or the information lost is the only possible optimization of the control communication system. Minimum error variance or deviation is, therefore, desired for a Gaussian noise source (Equation 5.3). In the more general case of a bandlimited channel with additive Gaussian white noise, the capacity is determined by the Shannon-Hartley Theorem:

$$C = B \log(1 + S/N) \quad \text{(Equation 5.19)}$$

for bandwidth B and average signal (S) and noise (N) power

A large bandwidth and signal-to-noise ratio (SNR) is desired in order to reach the greatest capacity for the channel. This theorem also indicates that a noiseless channel has infinite capacity. To reach the limiting rate of transmission of Equation 5.19, the source must approximate bandlimited white noise (i.e. colored noise) in all statistical properties. This ideal signalling scheme using noiselike signals approaches the channel capacity as the transmission delay and number of signals approaches infinity. However, in practice, we seldom try to achieve the maximum theoretical rate of transmission over the analog portion of a channel; rather, we keep this portion of the system reasonably simple. [Shannon]

By Shannon's Fundamental Theorem, the capacity for a noisy channel determines the theoretical upper limit to the system's rate of information transfer with arbitrarily small decision error. If the entropy of a source is less than or equal to the system's capacity ($\mathcal{H}(X) \leq C$), then there exists an encoding scheme for transmission across the channel which achieves an arbitrarily small probability of error. This is possible by sending the information in a redundant form and performing a statistical analysis on the different received versions of the message. This reduction in decision error causes a subsequent reduction in the lost information due to noise (i.e. $\mathcal{H}(X|Y) \rightarrow 0$) and, hence, an increase in the rate of transmission for the channel (i.e. $R \rightarrow \mathcal{H}(X)$). However, these benefits are at a cost of increased complexity and either: hardware for physical redundancy, or delay for repeated messages over the same channel. The cost of errorless transmission is infinite communication channels or infinite delay time. Hence, it is not possible to transmit information over a noisy channel without some probability of error due. If the source entropy is greater than the system's capacity, then information of an amount $\mathcal{H}(X|Y) \geq \mathcal{H}(X) - C$ is necessarily lost during transmission due to the definition of channel capacity. Errorless transmission is not theoretically possible in this case. In conclusion, a system designer always tries to optimize the rate of transmission to the channel's capacity by maximizing source information and by minimizing information losses due to interference through redundancy encoding. Shannon further adds:

> An approximation to the ideal would have the property that if the signal is altered in a reasonable way by the noise, the original can still be recovered. This is accomplished at the cost of a certain amount of redundancy in the coding. If the source already has a certain redundancy..., this redundancy will help combat noise. For example, in a noiseless telegraph channel one could save about 50% in time by proper encoding of the messages. This is not done and most of the redundancy of English remains in the channel symbols. This has the advantage, however, of allowing considerable noise in the channel. A sizable fraction of the letters can be received incorrectly and still be reconstructed by the context. In fact this is probably not a bad approximation to the ideal ... [Shannon]

5.5.1. Capacity of Redundant Structures for Fault-Tolerance

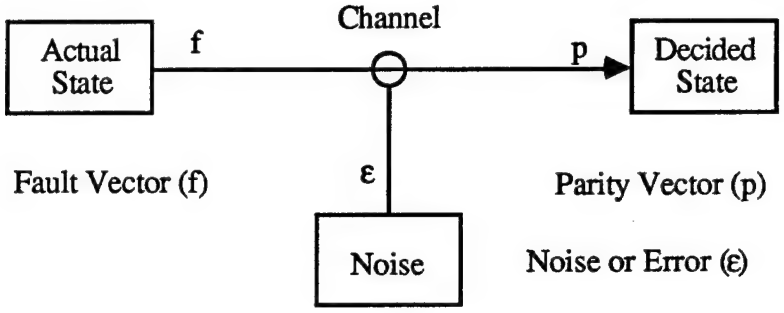


Figure 5.4 System State Decision or Information Channel

Here, the fault-tolerance of a redundant control structure in the presence of noise is evaluated (Figure 5.4). In this context, a redundant structure can be considered the channel which attempts to correctly determine or communicate the current state of the system (S) while contending with error or noise sources inherent within the decision. The system states and error sources possible for a redundant structure can be identified by a decision tree (e.g. Figure 4.18 and 4.30). This decision tree also represents explicitly the discrete communication or information channel for a redundant structure where: the input (X) is the prior information, the output (Y) is the system states, and the channel is the decision paths between input and output as dictated by the conditional knowledge of the FDI scheme. Due to decision errors in the FDI scheme, it is not possible to completely know the current system state by any operation upon the parity vector and information can be lost. The certainty of these decisions (min $\mathcal{H}(Y|X)$), the granularity or number of the system states (max $\mathcal{H}(Y)$), and the extent of our a priori knowledge (max $\mathcal{H}(X)$) determines the capacity (C) of the system for fault-tolerance (Equations 5.17, 5.18):

$$C = \max R = \max (\mathcal{H}(X) - \mathcal{H}(X|Y)) = \max(\mathcal{H}(Y) - \mathcal{H}(Y|X)) \Rightarrow$$
$$\max \mathcal{H}(Y), \max \mathcal{H}(Y), \text{ and } \min \mathcal{H}(Y|X)$$

The rate of information transmission (R) across the discrete channel is optimized by maximizing the mutual information between the input and output states. First, the extent of our a priori or input knowledge $\mathfrak{H}(X)$ is maximized. The entropy of the exponential reliability distribution is defined by the MTBF (Equation 5.4); any increase in the MTBF causes a logarithmic increase in the input knowledge. Hence, a more reliable control structure with a greater MTBF is desired. Second, system or output knowledge $\mathfrak{H}(Y)$ is maximized by increasing the granularity or number of the output system states (see Section 5.1. on entropy of discrete event sets). In Section 5.6.1., we shall find that redundancy provides this increase. However, the gains of this additional knowledge cannot be realized (and can even be at a detriment) if it is accompanied by poor utilization or transmission losses. The channel loss or uncertainty of the FDI scheme is minimized by approaching the ideal, matched transmission scheme where: $\mathfrak{H}(X|Y) = \mathfrak{H}(Y|X) = 0$ and $R = \mathfrak{H}(X) = \mathfrak{H}(Y)$. This corresponds to two possible ideal FDI schemes for redundant structures: the perfect-case of errorless decision, where $p00 = p11 = 1$ and $p01 = p10 = 0$; and the worst-case of complete decision error, where $p00 = p11 = 0$ and $p01 = p10 = 1$. Proper utilization of a redundant structure would also minimize the error variance of the controlled parameter (Equation 5.18), which we shall find corresponds with the perfect-case of errorless decision (Section 6.2). A large failure signal-to-noise ratio (SNR) is required in order to approach the perfect-case. In conclusion, the capacity or optimal rate of information transmission of a redundant structure for fault-tolerance is reached by utilizing a highly reliable control structure at the greatest level of redundancy while maintaining near-perfect FDI at all levels of operation. In practice, the capacity is never reached due to cost and other limitations not included within an analysis of information transmission. The key is to strive for higher transmission rates through reliability, redundancy, or better FDI performance while minimizing any important cost functions.

5.6. Entropy Analysis of Redundant Structures

As an example entropy analysis related to our study, redundant control structures will be examined and compared with respect to a system or joint entropy $\mathfrak{H}_{system}(t)$ which is defined by the entropy of the system state $\mathfrak{H}(S)$ and the conditioned error function $\mathfrak{H}(\varepsilon)$ for a given mission time (t). A table of the conditional error entropy $\mathfrak{H}(\varepsilon)$ for given system states has been compiled in Figure 5.5 to simplify these formulations. A redundant structure operated with a FDI scheme (e.g. the DDRS and TRS of Chapter 4) can be further analyzed with respect to the rate of information transmission for the FDI decision channel. These two system entropies represent the a priori uncertainty inherent within a redundant structure for a given time t of the mission. A control structure with a decision scheme of maximum rate and minimum error variance is optimal with respect to entropy (Section 5.5. and 5.5.1).

A table of the conditional error entropy $\mathfrak{H}(\varepsilon)$ is presented below for each possible system state of the redundant structures which are analyzed. The probability distribution for the error is derived in Section 3.1.1. for a system state with n failed and m working structures (Equation 3.3 -3.7). The probability distribution for a single working control structure is represented as Gaussian with zero mean and standard deviation σ (σ = 0.3276%FS, Figure 2.4). The error distribution for a redundant structure is represented as either: Uniform with a base width of α, or Gaussian with zero mean and standard deviation σ_S. The entropy $\mathfrak{H}(\varepsilon)$ for these distributions is derived in Equations 5.2 and 5.3. The conditional error function when three structures are working is arbitrarily chosen as the measure function m(x) and therefore its entropy will represent zero uncertainty. The conditional error entropy with respect to this measure function is represented as $\mathfrak{H}_m(\varepsilon)$ in the table. Note that the entropy of corresponding system states is reduced with each level of redundancy.

System State	n	m	Probability Density		$\mathcal{H}(\varepsilon)$	$\mathcal{H}_m(\varepsilon)$
Single Structure, Working	0	1	Gaussian	$\sigma_s = \sigma$	$\log(\sigma\sqrt{2\pi e})$	0.55
Single Structure, Not Working	1	0	Uniform	$\alpha = 2\,FS$	$\log(2\,FS)$	5.54
Dual Structure, Both Working	0	2	Gaussian	$\sigma_s = \sigma/\sqrt{2}$	$\log(\sigma\sqrt{\pi e})$	0.20
Dual Structure, One Working	1	1	Uniform	$\alpha = FS$	$\log(FS)$	4.85
Dual Structure, None Working	2	0	Gaussian	$\sigma_s = FS/\sqrt{6}$	$\log(FS\sqrt{\pi e/3})$	5.37
Triple Structure, All Working	0	3	Gaussian	$\sigma_s = \sigma/\sqrt{3}$	$\log(\sigma\sqrt{2\pi e/3})$	0
Triple Structure, Two Working	1	2	Uniform	$\alpha = 2\,FS/3$	$\log(2\,FS/3)$	4.45
Triple Structure, One Working	2	1	Gaussian	$\sigma_s = FS\sqrt{2}/\sqrt{27}$	$\log(2FS\sqrt{\pi e/27})$	4.97
Triple Structure, None Working	3	0	Gaussian	$\sigma_s = FS/3$	$\log(FS\sqrt{2\pi e/9})$	5.17

Figure 5.5 Error Entropy For Each System State

In Appendix B, an example entropy analysis for a single and dual redundant control structure with respect to the failure time and conditioned error functions for a given mission length T is also provided. This analysis examines the use of the continuous failure time function as the basis for system uncertainty. Results are similar to those found in this section but are much more difficult to reach.

5.6.1. Entropy Analysis of Redundant Structures without FDI

This section examines the entropy of redundant structures which do not perform fault detection and isolation. A system or joint entropy $\mathcal{H}_{system}(t)$, which represents the a priori uncertainty inherent within a redundant structure for a given time t of the mission, is formulated from the exponential reliability distribution and the Gaussian error function conditioned upon the system state of the structure. For example, a dual redundant structure without any FDI scheme has a discrete set of system states: both structures working, single fault of either structure, and both structures inoperative. The size of the event set is further increased with the number (N) of redundant structures. It is assumed that no decision is made regarding the current state of the system and that all control structures are included within the voting/estimation algorithm at any given time t of the mission. A FDI and reconfiguration scheme would add more possible states/events for the redundant structure as dictated by the decision trees presented in Chapter 4 (see Figures 4.18 and 4.30). System entropy is formulated as the joint entropy of the discrete set S of system states and the continuous Gaussian or Uniform density of the conditional error ε (Figure 5.5):

$$\mathcal{H}_{system}(t) = \mathcal{H}(\varepsilon,S\,|t) = \mathcal{H}(S\,|t) + \mathcal{H}(\varepsilon\,|S,t) \qquad \text{(Equation 5.20)}$$

The entropy of the system state set $\mathcal{H}(S\,|t)$ is formulated directly from Shannon's equation (Equation 5.1) for discrete events and exhibits a characteristic, "humped" curve. The entropy peaks just before reaching the MTBF for a single structure when all events are equally certain and subsequently approaches zero as we become more and more certain that all structures have failed ($Q(\infty)=1$). Thus, the contribution to the system entropy becomes negligible with large mission times. The entropy of the system state set increases monotonically with the level of redundancy due to the increased size of the structure event set. The failure rate of the example reliability budget (0.000142, Figure 3.7) is used in producing the following figures.

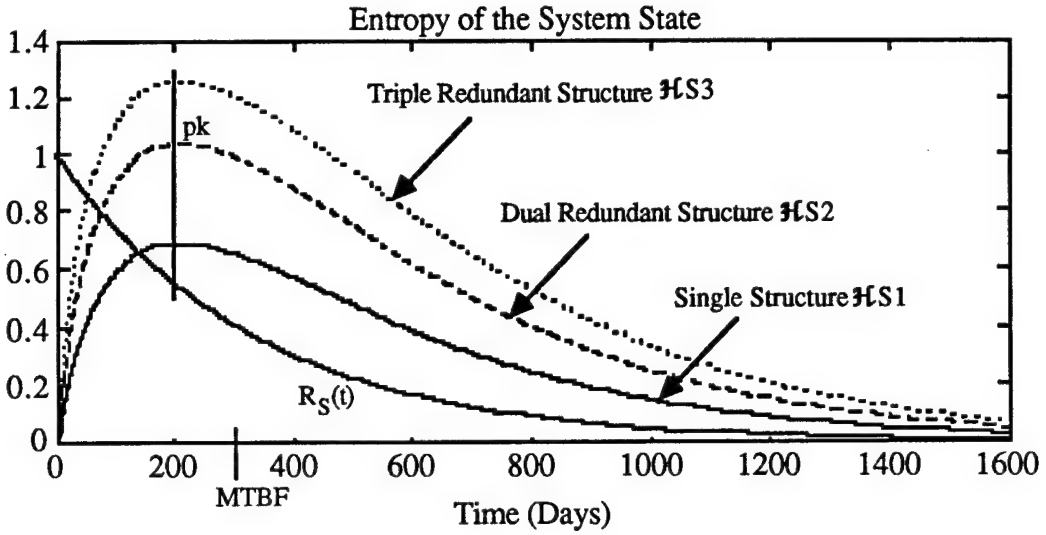


Figure 5.6 Entropy of the System State for Redundant Structures

Single Structure

$$\mathcal{H}(S\,|t) = -R_S(t) \log R_S(t) - (1 - R_S(t)) \log (1 - R_S(t)) \qquad \text{(Equation 5.21)}$$

Dual Redundant Structure

$$\mathcal{H}(S\,|t) = -R_S^2(t) \log R_S^2(t) - 2\,R_S(t)\,Q_S(t) \log 2\,R_S(t)\,Q_S(t) - Q_S^2(t) \log Q_S^2(t) \qquad \text{(Equation 5.22)}$$

Triple Redundant Structure

$$\mathcal{H}(S\,|t) = -R_S^3(t) \log R_S^3(t) - 3\,Q_S(t)\,R_S^2(t) \log 3\,Q_S(t)\,R_S^2(t) - 3\,R_S(t)\,Q_S^2(t) \log 3\,R_S(t)\,Q_S^2(t) - Q_S^3(t) \log Q_S^3(t) \qquad \text{(Equation 5.23)}$$

The mean conditional entropy $\mathcal{H}(\varepsilon \mid S,t)$ of the error function is defined as the uncertainty of the error for a given state averaged over all possible states of the structure (Equations 5.24 - 5.26). The entropy of the error function for each system state is tabulated in Figure 5.5 with respect to a measure function m(x). The conditional error function when three structures are working is arbitrarily chosen as the measure function m(x) and therefore its entropy will represent zero uncertainty. In Figure 5.7, the mean conditional entropy for the error monotonically increases over the mission time from the initial system state where all structures are working (Gaussian with tight variance) to the worst-case system state where all structures have failed (Uniform over fullscale range). For the majority of the mission, the mean conditional entropy is found to increase with additional levels of redundancy because of the corrupting effect of any single controller failure to the estimation algorithm. However, redundancy does afford a lower initial and final entropy due to the reduced variance of the error function upon averaging the controlled parameter. Mean conditional entropy necessarily dominates the joint or system entropy $\mathcal{H}_{system}(t)$ due to the continuous nature of the error function (Figure 5.8).

Single Structure

$$\mathcal{H}(\varepsilon \mid S,t) = R_S(t)\,\mathcal{H}(\varepsilon \mid \text{Working}) + Q_S(t)\,\mathcal{H}(\varepsilon \mid \text{Not Working}) = R_S(t) * 0.55 + Q_S(t) * 5.54$$

Dual Redundant Structure

$$\mathcal{H}(\varepsilon \mid S,t) = R_S^2(t)\,\mathcal{H}(\varepsilon \mid \text{Both Working}) + 2\,R_S(t)\,Q_S(t)\,\mathcal{H}(\varepsilon \mid \text{One Working}) + Q_S^2(t)\,\mathcal{H}(\varepsilon \mid \text{None Working})$$

$$\mathcal{H}(\varepsilon \mid S,t) = R_S^2(t) * 0.20 + 2\,R_S(t)\,Q_S(t) * 4.85 + Q_S^2(t) * 5.37$$

Triple Redundant Structure

$$\mathcal{H}(\varepsilon \mid S,t) = 3\,Q_S(t)\,R_S^2(t) * 4.45 + 3\,R_S(t)\,Q_S^2(t) * 4.97 + Q_S^3(t) * 5.17$$

(Equations 5.24 - 5.26)

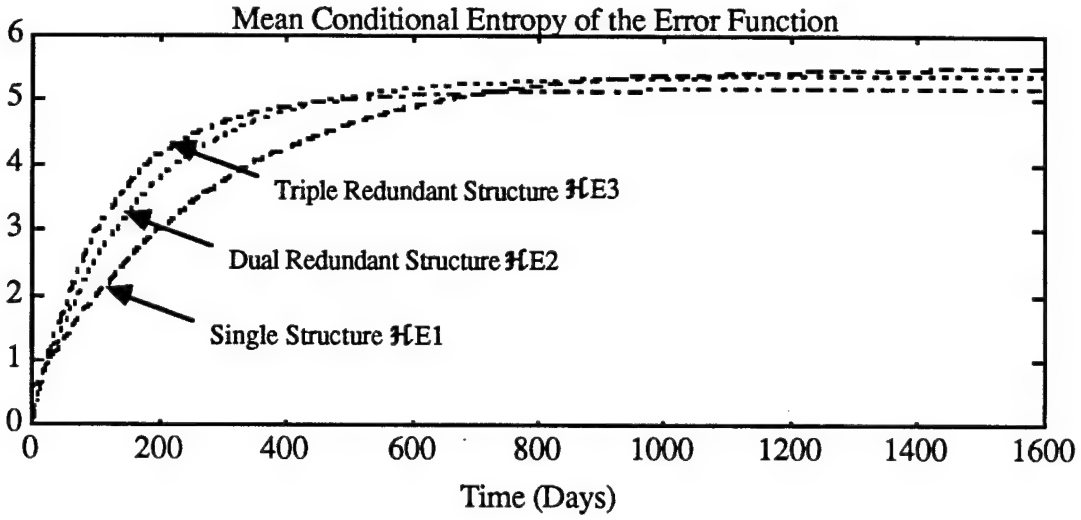


Figure 5.7 Mean Conditional Entropy of the Error Function

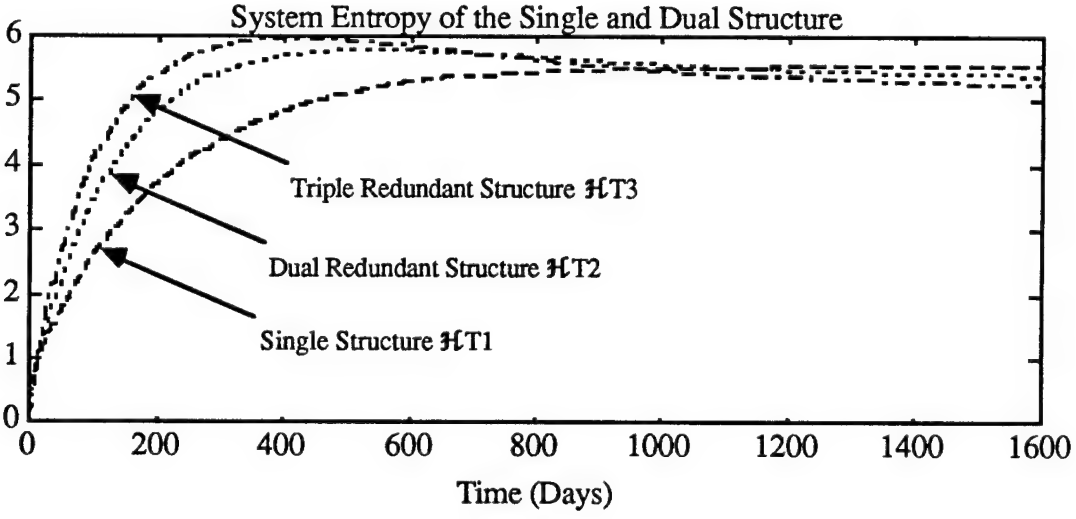


Figure 5.8 Joint or System Entropy of the Control Structure

5.6.2. Entropy Analysis of a Single Control Structure with Fault Detection

In this section, the relative merit of a fault detection scheme for a single control structure is examined. In the exercises of this thesis, it has been assumed that system shutdown is not a possible system state. Hence, no matter what decision is made by a fault detection scheme, the control structure will be utilized in all estimates of the controlled parameter for the length of the mission. The only benefit of a fault detection scheme in this situation is to alert the operator of possible failure. Three fault detection schemes of differing performance are examined with respect to entropy and information transmission: the perfect case of errorless detection, the worst case of complete misinformation, and the poor or noisy case which results in no information. The failure rate of the example reliability budget (0.000142, Figure 3.7) and the conditional error entropies of Figure 5.5 are used in producing the following figures. In each case, the following are derived and compared:

1) Outcome entropy $\mathcal{H}Y1^*$, mean conditional entropy $\mathcal{H}C1^*$, and rate of information transmission $RT1^* = \mathcal{H}Y1^* - \mathcal{H}C1^*$ for the FDI channel or decision.

2) System state entropy $\mathcal{H}S1^*$, mean conditional entropy of the estimation error $\mathcal{H}E1^*$, and system or joint entropy $\mathcal{H}T1^* = \mathcal{H}S1^* + \mathcal{H}E1^*$.

A control structure with a decision scheme of maximum rate and minimum error variance is optimal with respect to entropy (Section 5.5. and 5.5.1).

Note: * represents a suffix (e.g. pc, wc, poor) used to distinguish the results for different FDI schemes.

Note: Results for a structure without FDI is represented without a suffix.

Perfect Fault Detection ($P_{00} = P_{11} = 1, P_{01} = P_{10} = 0$)

$$\mathcal{H}Y1^* = - \text{pr}\{\text{decide structure working}\} \log (\text{pr}\{\text{decide structure working}\}) - \text{pr}\{\text{decide structure failed}\} \log (\text{pr}\{\text{decide structure failed}\})$$

$$\mathcal{H}Y1pc = - (R P_{00} + Q P_{01}) \log (R P_{00} + Q P_{01}) - (R P_{10} + Q P_{11}) \log(R P_{10} + Q P_{11})$$

$$\mathcal{H}Y1pc = - R \log R - Q \log Q = \mathcal{H}S1$$

$$\mathcal{H}C1pc = - R (P_{00} \log P_{00} + P_{10} \log P_{10}) - Q (P_{11} \log P_{11} + P_{01} \log P_{01}) = 0$$

$$RT1pc = \mathcal{H}(Y) - \mathcal{H}(Y|X) = \mathcal{H}Y1pc - \mathcal{H}C1pc = \mathcal{H}S1$$

(Equations 5.27 - 5.29)

Worst Fault Detection ($P_{00} = P_{11} = 0, P_{01} = P_{10} = 1$)

$$\mathcal{H}Y1wc = - R \log R - Q \log Q = \mathcal{H}S1$$

$$\mathcal{H}C1wc = 0; \quad RT1wc = \mathcal{H}S1$$

(Equations 5.30 - 5.32)

Poor Fault Detection ($P_{00} = P_{11} = P_{01} = P_{10} = 0.5$)

$$\mathcal{H}Y1poor = \log 2 \leq \mathcal{H}S1$$

$$\mathcal{H}C1poor = \log 2; \quad RT1poor = 0$$

(Equations 5.33 - 5.35)

Single Structure with any FD Scheme and No Shutdown

$$\mathcal{H}S1^* = -R\,(P_{00} + P_{10}) \log(R\,(P_{00} + P_{10})) - Q\,(P_{11} + P_{01}) \log(Q\,(P_{11} + P_{01}))$$

$$\mathcal{H}S1^* = -R \log R - Q \log Q = \mathcal{H}S1$$

$$\mathcal{H}E1^* = R\,\mathcal{H}(\varepsilon \mid \text{Working}) - Q\,\mathcal{H}(\varepsilon \mid \text{Failed}) = R * 0.55 + Q * 5.54 = \mathcal{H}E1$$

$$\mathcal{H}T1^* = \mathcal{H}T1$$

(Equations 5.36, 5.37)

The inclusion of any type of fault detection scheme has no effect on the mean conditional entropy of the error because the control structure is utilized irregardless of the decided system state. Hence, system performance (in terms of the error variance of the controlled parameter) is independent of the fault detection scheme. Also, perfect and worst case fault detection cannot be distinguished from each other; nor from the case without fault detection. However, it is indicated that a poor fault detection scheme is not acceptable due to its zero rate of information transmission (i.e. the decision is independent from the system and is, therefore, equally informative as flipping a coin). The conclusion from this analysis is that no fault detection scheme should be utilized for a single control structure without shutdown capability. Obviously, this conclusion is a bit premature without some analysis of cost functions other than error variance (e.g. operator safety, cost of implementation). This conclusion is quite common for any consumable process which is simply discarded or replaced upon failure. For some applications, however, the cost of operator safety dictates the necessity of quick detection of system failure so that the operator may respond with protective measures. The predicted mission outcome from this analysis is that the control structure will operate with the specified variance (σ^2) until the MTBF. Therefore, mission length must be less than the MTBF and would optimally be set at the time of maximum system state entropy (i.e. the hump of Figure 5.6).

The relative merit of a fault detection scheme for a single control structure is now examined where system shutdown is a possible system state. System shutdown is initiated immediately upon detection of a fault. Here, the benefit of a fault detection scheme is to avoid faulty performance or product by simply ending the mission. The tabulation of mean conditional entropy of the error function (Figure 5.5) must be expanded to cover these additional states (Figure 5.9). Note that error entropy is zero during system shutdown. Decision entropies and information rates for the FDI channel remain unchanged since the two decisions (structure working, structure failed) are unchanged.

System State	p(S)	$\mathcal{H}_m(\varepsilon)$
Normal Operation	$R\,P_{00}$	0.55
System Shutdown	$R\,P_{10} + Q\,P_{11}$	0
Missed Detection	$Q\,P_{01}$	5.54

Figure 5.9 Error Entropy For System States

Three fault detection schemes of differing performance are examined with respect to entropy and information transmission: the perfect case of errorless detection, the worst case of complete misinformation, and the poor or noisy case which results in no information.

Perfect Fault Detection ($P_{00} = P_{11} = 1, P_{01} = P_{10} = 0$)

$$\mathcal{H}S1pc = -R\,P_{00}\log(R\,P_{00}) - (R\,P_{10} + Q\,P_{11})\log(R\,P_{10} + Q\,P_{11}) - Q\,P_{01}\log(Q\,P_{01})$$

$$\mathcal{H}S1pc = -R\log R - Q\log Q = \mathcal{H}S1$$

$$\mathcal{H}E1pc = R\,P_{00}\,\mathcal{H}(\varepsilon \mid \text{Working}) - (R\,P_{10} + Q\,P_{11})\,\mathcal{H}(\varepsilon \mid \text{Shutdown}) - Q\,P_{01}\,\mathcal{H}(\varepsilon \mid \text{Failed})$$

$$\mathcal{H}E1pc = R * 0.55 \approx 0$$

(Equations 5.38, 5.39)

Worst Fault Detection ($P_{00} = P_{11} = 0, P_{01} = P_{10} = 1$)

$$\mathcal{H}S1wc = -R \log R - Q \log Q = \mathcal{H}S1$$

$$\mathcal{H}E1wc = Q * 5.54 \approx \mathcal{H}S1$$

(Equations 5.40, 5.41)

Poor Fault Detection ($P_{00} = P_{11} = P_{01} = P_{10} = 0.5$)

$$\mathcal{H}S1poor = -0.5 R \log R - 0.5 Q \log Q + \log 2 > \mathcal{H}S1$$

$$\mathcal{H}E1poor = 0.5 * (R * 0.55 + Q * 5.54) = 1/2\ \mathcal{H}E1$$

(Equations 5.42, 5.43)

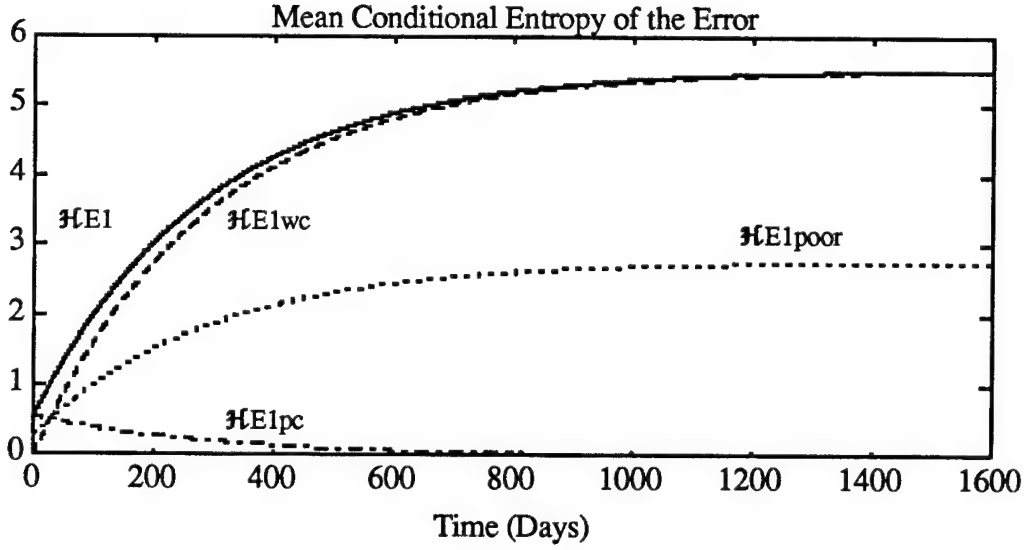


Figure 5.10 Error Entropy for Structure with Shutdown

In this example formulation, the perfect and worst case of fault detection are again indistinguishable in their rate of information transmission and poor fault detection is found to have zero rate of transmission. With the new set of error entropies for the additional system state of shutdown (Figure 5.9), the perfect case of errorless fault detection is determined to provide the smallest average conditional entropy for estimation error. The conclusion from this analysis is that perfect fault detection is optimal for a single control structure with shutdown capability. However, this analysis also indicates that any fault detection scheme (even worst case) is preferable to none. Initially, the error entropy for the worst case detection scheme is actually the smallest at zero. This is because no cost is assigned to the case of false alarm. The worst case scheme of misinformation would immediately stop the mission due to its ignorance. The following analysis addresses this problem. Here, the system state of false alarm is given the same weight as missed detection in the tabulation of entropy for the error function (Figure 5.11).

System State	p(S)	$\mathfrak{H}_m(\varepsilon)$
Normal Operation	$R P_{00}$	0.55
False Alarm	$R P_{10}$	5.54
Fault Detection	$Q P_{11}$	0
Missed Detection	$Q P_{01}$	5.54

Figure 5.11 Error Entropy For System States

Worst Fault Detection: $\mathfrak{H}E1wc = 5.54 > \mathfrak{H}S1$ (Equation 5.44)

Poor Fault Detection: $\mathfrak{H}E1poor = 0.5 * (R * (0.55 + 5.54) + Q * 5.54)$ (Equation 5.45)

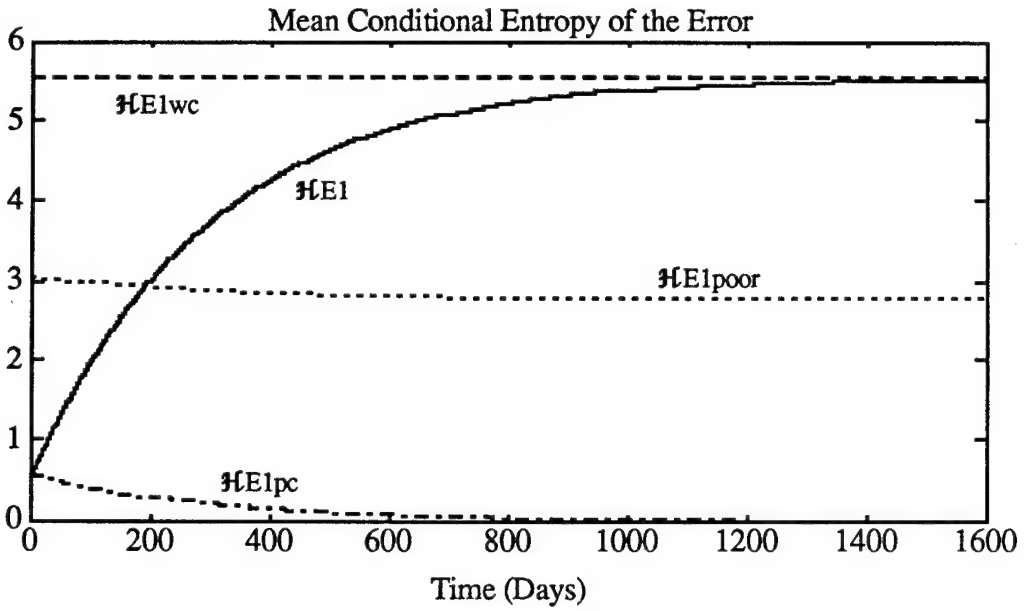


Figure 5.12 Error Entropy for Structure with Shutdown and False Alarm Cost

Perfect fault detection remains optimal. The only result modified is that the mean conditional entropy of the error is increased for the poor and worst cases of fault detection (Equations 5.54, 5.55). Initially, a structure with a fault detection scheme can be considered less optimal than a structure without FDI. As the mission progresses, a fault detection scheme becomes desirable. The greater the decision error for the detection scheme, the further in the mission for the scheme to become useful. The perfect detection scheme would be utilized immediately. The worst case scheme of misinformation is never utilized. The poor or noisy fault detection scheme is only acceptable after the probability of a failure is already high. This mimics the threshold variation which occurs with a fault detection scheme based on the Bayes criterion. The threshold is set very high initially (when the reliability is very high) such that false alarms are minimized. As the mission progresses, the threshold is reduced to zero in order to sensitize the test to fault occurrences. Therefore, this cost analysis allows determination of whether a fault detection scheme is acceptable and, if so, when during the mission it should be utilized.

5.6.3. Entropy Analysis of Dual Redundant Structures

In this section, the relative merit of a fault detection scheme for redundant control structures is examined. In the exercises of this thesis, it has been assumed that system shutdown is not a possible system state. Hence, no matter what decision branch is followed by a fault detection scheme, at least one control structure will be utilized in the estimates of the controlled parameter for the length of the mission. The benefit of a fault detection scheme in this situation is to alert the operator and to isolate any possible failure so that continuous operation can be maintained with the working controller. Many fault detection schemes of differing performance are examined with respect to entropy and information transmission. The failure rate of the example reliability budget (0.000142, Figure 3.7) and the conditional error entropies of Figure 5.5 are used in producing the following figures. In each case, the following are derived and compared:

1) Outcome entropy $\mathfrak{H}Y\#^*$, mean conditional entropy $\mathfrak{H}C\#^*$, and rate of information transmission $RT\#^* = \mathfrak{H}Y\#^* - \mathfrak{H}C\#^*$ for the FDI channel or decision.

2) System state entropy $\mathfrak{H}S\#^*$, mean conditional entropy of the estimation error $\mathfrak{H}E\#^*$, and system or joint entropy $\mathfrak{H}\#^* = \mathfrak{H}S\#^* + \mathfrak{H}E\#^*$.

A control structure with a decision scheme of maximum rate and minimum error variance is optimal with respect to entropy (Section 5.5. and 5.5.1).

Note: * represents a suffix (e.g. pc, wc, poor) used to distinguish the results for different FDI schemes. Results for a redundant structure without FDI is represented without this suffix.

Note: # represents a numerical suffix (e.g. 1, 2, 3) used to distinguish the results for a different number N of redundant structures.

First, a dual structure without simplex FDI schemes (Figure 4.18) is examined for four cases of duplex fault detection: the optimized case of the Bayes criterion, the static threshold case of the Neyman-Pearson criterion, the worst case of complete misinformation, and the poor or noisy case which results in no information. Only two decisions or outcomes are possible (both working, dual or single fault) because no simplex FDI is implemented. A failure SNR of five (used in previous exercises) is assumed. The conditional probability of a hidden dual fault or common bias given that a dual fault has occurred is represented here as P_{DF}. Also, refer to Equations 4.20 - 4.24 for the system state probabilities.

$$\mathcal{H}Y2^* = - \text{pr\{decide both working\}} \log (\text{pr\{decide both working\}}) - \text{pr\{decide dual or single fault\}} \log (\text{pr\{decide dual or single fault\}})$$

$$\mathcal{H}Y2^* = - (R^2 P_{00} + 2 R Q P_{01} + Q^2 P_{DF} P_{00} + Q^2 (1 - P_{DF}) P_{01}) * \log (R^2 P_{00} + 2 R Q P_{01} + Q^2 P_{DF} P_{00} + Q^2 (1 - P_{DF}) P_{01}) - (R^2 P_{10} + 2 R Q P_{11} + Q^2 P_{DF} P_{10} + Q^2 (1 - P_{DF}) P_{11}) * \log (R^2 P_{10} + 2 R Q P_{11} + Q^2 P_{DF} P_{10} + Q^2 (1 - P_{DF}) P_{11})$$

$$\mathcal{H}C2^* = - R^2 (P_{00} \log P_{00} + P_{10} \log P_{10}) - 2 R Q (P_{11} \log P_{11} + P_{01} \log P_{01}) - Q^2 (P_{DF} P_{00} \log P_{DF} P_{00} + P_{DF} P_{10} \log P_{DF} P_{10} + (1 - P_{DF}) P_{11} \log ((1 - P_{DF}) P_{11}) + (1 - P_{DF}) P_{01} \log ((1 - P_{DF}) P_{01}))$$

$$\mathcal{H}S2^* = - P_{S1} \log P_{S1} - P_{S2} \log P_{S2} - P_{S3} \log P_{S3} - P_{S4} \log P_{S4} - P_{S5} \log P_{S5}$$

$$\mathcal{H}E2^* = P_{S1} \mathcal{H}(\varepsilon \mid S1) + P_{S2} \mathcal{H}(\varepsilon \mid S2) + P_{S3} \mathcal{H}(\varepsilon \mid S3) + P_{S4} \mathcal{H}(\varepsilon \mid S4) + P_{S5} \mathcal{H}(\varepsilon \mid S5)$$

$$\mathcal{H}E2^* = P_{S1} * 0.2 + P_{S2} * 4.85 + P_{S3} * 5.37 + P_{S4} * 0.55 + P_{S5} * 5.54$$

(Equations 5.46 - 5.49)

Perfect Duplex Fault Detection ($P_{00} = P_{11} = 1, P_{01} = P_{10} = P_{DF} = 0$)

$$\mathcal{H}Y2pc = - R^2 \log R^2 - (2 R Q + Q^2) \log (2 R Q + Q^2)$$

$$\mathcal{H}C2pc = 0; \quad RT2pc = \mathcal{H}Y2pc$$

$$\mathcal{H}S2pc = - R^2 \log R^2 - R Q \log R Q - (R Q + Q^2) \log (R Q + Q^2)$$

$$\mathcal{H}E2pc = R^2 * 0.2 + R Q * 0.55 + (R Q + Q^2) * 5.54$$

(Equations 5.50 - 5.54)

Worst Duplex Fault Detection ($P_{00} = P_{11} = P_{DF} = 0, P_{01} = P_{10} = 1$)

$$\mathcal{H}Y2wc = (2 R Q + Q^2) \log (2 R Q + Q^2) - R^2 \log R^2$$

$$\mathcal{H}C2wc = 0; \quad RT2wc = \mathcal{H}Y2wc$$

$$\mathcal{H}S2wc = - 2 R Q \log (2 R Q) - Q^2 \log Q^2 - R^2 \log R^2$$

$$\mathcal{H}E2wc = 2 R Q * 4.85 + Q^2 * 5.37 + R^2 * 0.55$$

(Equations 5.55 - 5.59)

Poor Fault Detection ($P_{00} = P_{11} = P_{01} = P_{10} = 0.5, P_{DF} = 0$)

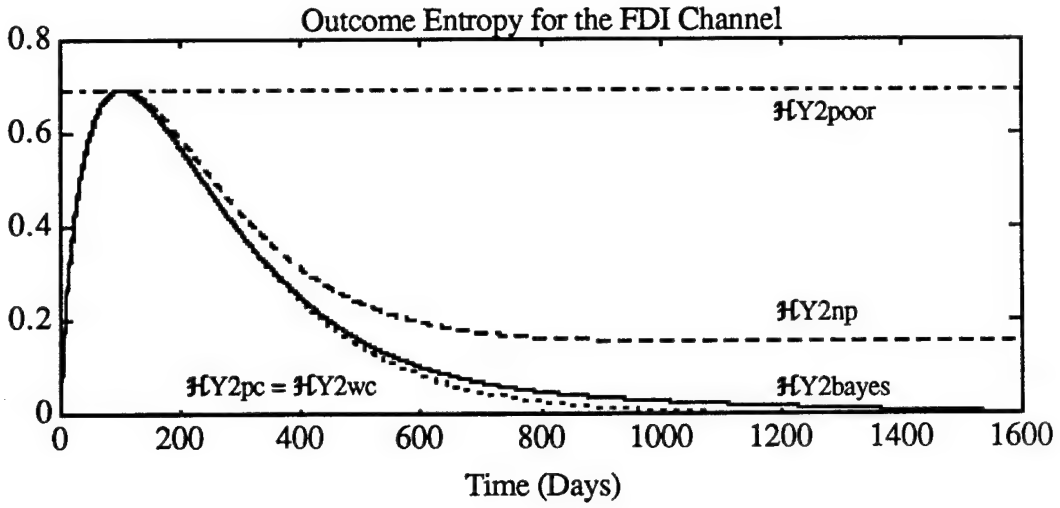
$$\mathcal{H}Y2poor = - (R^2 + 2 R Q + Q^2) * \log (0.5 * (R^2 + 2 R Q + Q^2)) = \log 2$$

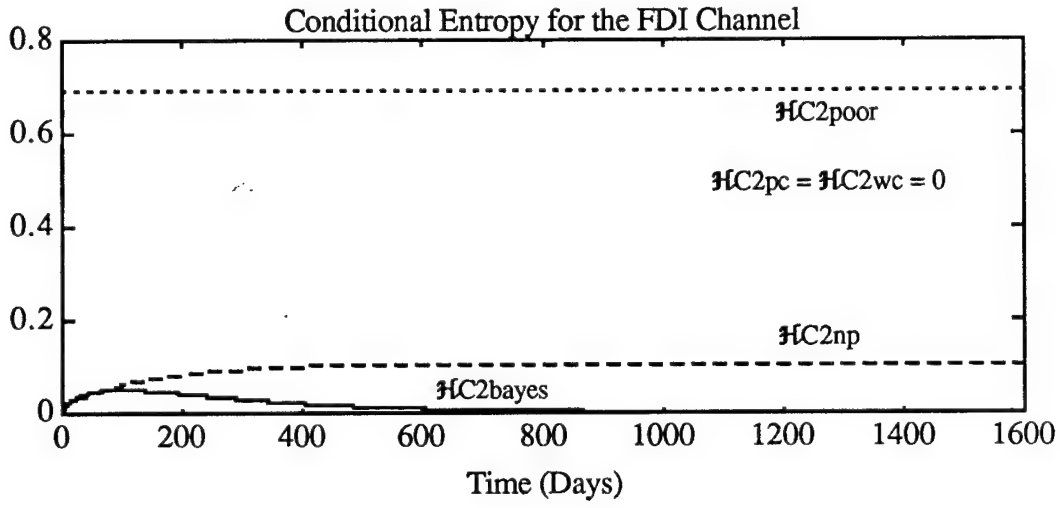
$$\mathcal{H}C2poor = \log 2; \quad RT2poor = \mathbf{0}$$

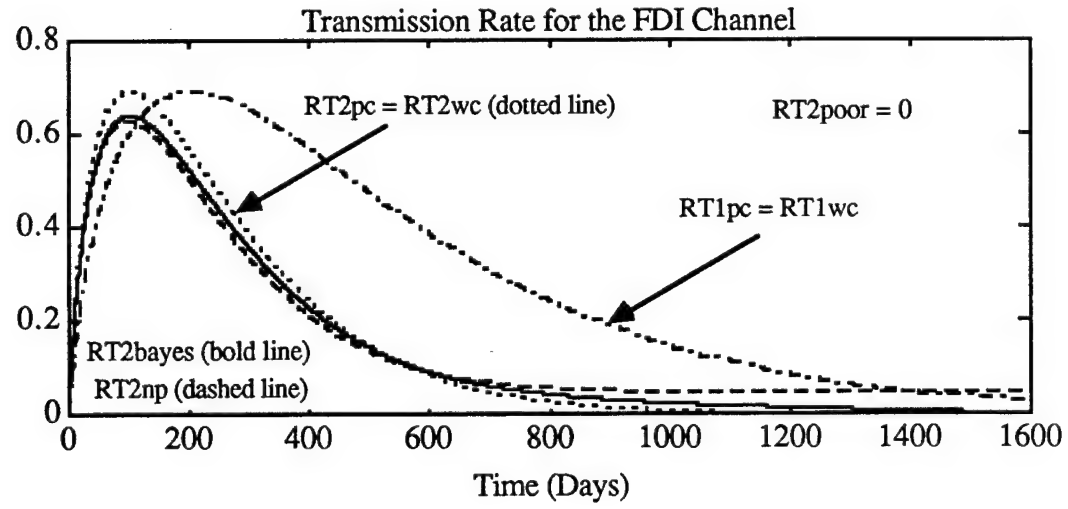
$$\mathcal{H}S2poor = - 0.5 * R^2 \log(0.5 * R^2) - R Q \log (R Q) - 0.5 * Q^2 \log(0.5 * Q^2) - 0.5 * (R^2 + R Q) \log(0.5 * (R^2 + R Q)) - 0.5 * (Q^2 + R Q) \log(0.5 * (Q^2 + R Q))$$

$$\mathcal{H}E2poor = R^2 * 0.1 + R Q * 4.85 + Q^2 * 2.685 + (R^2 + R Q) * 0.275 + (Q^2 + R Q) * 2.77$$

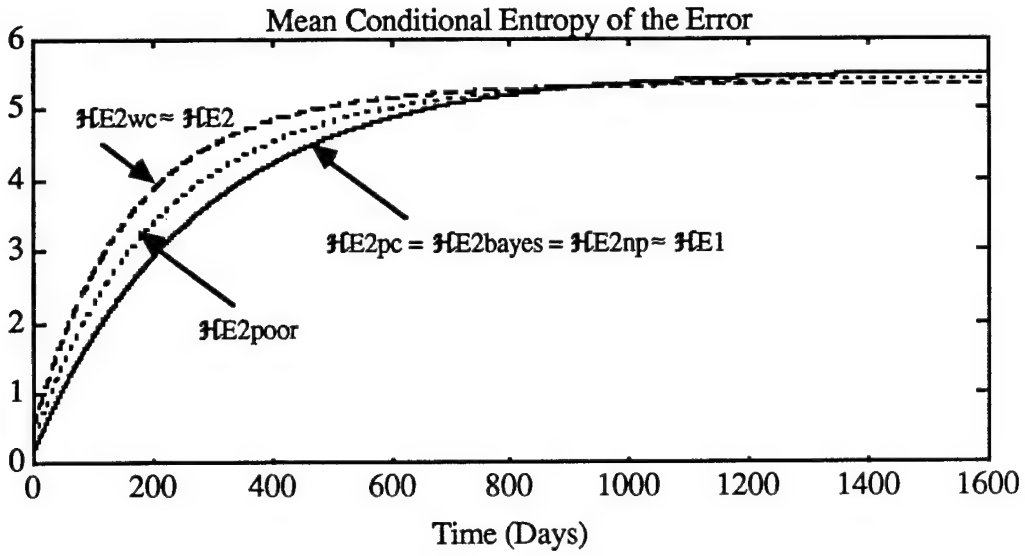
(Equations 5.60 - 5.64)

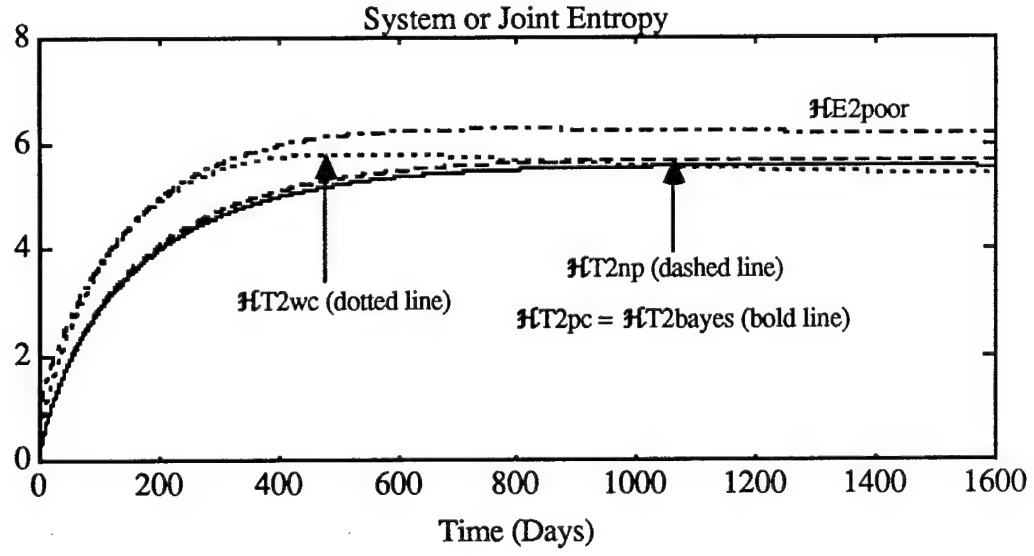






Figures 5.13 - 5.15





Figures 5.16, 5.17

Results

	Outcome Information	poor = log 2 > np > bayes > pc = wc
	Missing Information	poor = log 2 > np > bayes > pc = wc = 0
➡	Transmission Rate	pc = wc > bayes > np > poor = 0
➡	Error Entropy	wc > poor > pc = bayes = np
	System Entropy	poor > wc > np > pc = bayes

Perfect and worst case fault detection are found to provide the highest rate of information transmission, while poor or noisy fault detection has a zero transmission rate. The Bayes criterion allows a slightly higher information rate than the Neyman-Pearson (np) criterion, both of which are near optimal. Note the improvement of the Bayes criterion at reducing the amount of lost or missing information due to noise or error ($\mathcal{H}$C2bayes < $\mathcal{H}$C2np). In comparison with a single structure without shutdown, duplex fault detection has a higher transmission rate initially due to the additional outcome information and a lower rate beyond the MTBF due to the inability to distinguish between dual and single failures. Of course, the duplex scheme can incorporate these simplex schemes in order to improve its fault tolerance (see below).

Perfect, Bayes, and Neyman-Pearson fault detection provide the lowest mean conditional error entropy over the length of the mission. The mean error entropy for these schemes is less than or equal to the mean error entropy of a single structure ($\mathcal{H}$E1pc ≤ $\mathcal{H}$E1, Figure 5.16). Initially, they are improved due to the reduced error variance from the estimation average. The worst case scheme provides the highest mean error entropy and is approximately equal to the mean error entropy of the dual structure without fault detection ($\mathcal{H}$E2wc ≈ $\mathcal{H}$E2, Figure 5.16). Similar results hold for the system or joint entropy. System entropy for the Bayes criterion, however, is lower than that for the Neyman-Pearson criterion.

Therefore, a dual redundant structure with an errorless duplex test allows a higher rate of information and a lower mean error entropy over a single control structure (with or without fault detection) for short missions which end before the MTBF. Bayes detection is preferred over Neyman-Pearson. A dual structure without shutdown can achieve the same performance with or without worst case detection, but must strive for perfect case detection to improve upon the performance of a single structure.

A dual structure with two levels of fault detection (i.e. duplex and simplex FDI) is examined for three cases: the perfect case of errorless detection at both levels, the worst case of complete misinformation at both levels, and the poor or noisy case which results in no information. Three decisions or outcomes are possible (both working, single fault, and dual fault). Again, system shutdown is not considered as a possible system state. Additionally, one level must be given precedence over the other in order to resolve conflicts between the two levels of fault detection. The above results for a dual structure with only duplex fault detection can be considered comparable with the case of full FDI where duplex detection is given precedence and simplex detection is poor or noisy such that it provides no additional information. Simplex detection upon either single controller within the dual structure is independent from duplex detection upon the pair of controllers and simplex detection upon the other control structure. The conditional probabilities for the simplex detection scheme upon either single controller are represented as $P_{S\#\#}$ (e.g. P_{S10} = the probability of deciding a working structure is failed). However, simplex detection applied to the second control structure is dependent upon the results of the simplex detection applied to the first control structure and the duplex detection applied to the pair of control structures. The conditional probabilities for the simplex detection scheme applied to the second controller are represented as $P_{S(\#\#)(\#\#)\#}$ (e.g. $P_{S(10)(10)0}$ = the probability of deciding the second working controller is failed when the first working controller and the dual structure are considered failed). A property of mutually exclusive and exhaustive

events is that the sum of their probabilities must equal unity (e.g. $P_{S(10)(10)0} + P_{S(00)(10)0} = P_{S10} + P_{S00} = 1$). In the ideal detection schemes to be examined (perfect, worst, and poor), independence is assumed between duplex and simplex tests and, therefore, $P_{S(\#\#)(\#\#)\#} = P_{S\#\#}$. The failure rate of the example reliability budget (0.000142, Figure 3.7) and the conditional error entropies of Figure 5.5 are used in producing the following figures. A control structure with a decision scheme of maximum rate and minimum error variance is optimal with respect to entropy (Section 5.5. and 5.5.1). In each case, the following are derived and compared:

1) Outcome entropy $\mathfrak{H}$Y2F#*, mean conditional entropy $\mathfrak{H}$C2F#*, and rate of information transmission RT2F#* = $\mathfrak{H}$Y2F#* - $\mathfrak{H}$C2F#* for the FDI channel or decision.

2) System state entropy $\mathfrak{H}$S2F#*, mean conditional entropy of the estimation error $\mathfrak{H}$E2F#*, and system or joint entropy $\mathfrak{H}$2F#* = $\mathfrak{H}$S2F#* + $\mathfrak{H}$E2F#*.

Note: * represents a suffix (e.g. pc, wc, poor) used to distinguish the results for different FDI schemes. Results for a redundant structure without FDI is represented without this suffix.

Note: # represents the level of fault detection given precedence for conflict resolution (e.g. 2 indicates duplex detection has precedence, while 1 indicates simplex detection)

Note: The suffix F represents a redundant structure with full FDI at all levels.

$$\begin{aligned}\mathfrak{H}\text{Y2F\#*} = &- \text{pr\{decide both working\}} \log (\text{pr\{decide both working\}}) \\ &- \text{pr\{decide single fault\}} \log (\text{pr\{decide single fault\}}) \\ &- \text{pr\{decide dual fault\}} \log (\text{pr\{decide dual fault\}})\end{aligned}$$

$$\mathcal{H}Y2F2^* = - (R^2 P_{00} + 2 R Q P_{01} + Q^2 P_{DF} P_{00} + Q^2 (1 - P_{DF}) P_{01}) * \log (R^2 P_{00} + 2 R Q P_{01} + Q^2 P_{DF} P_{00} + Q^2 (1 - P_{DF}) P_{01})$$

$$- (R^2 P_{10} (1 - P_{S10} P_{S10101}) + 2 R Q P_{11} (1 - P_{S10} P_{S11101}) + (Q^2 P_{DF} P_{10} + Q^2 (1 - P_{DF}) P_{11}) (1 - P_{S11} P_{S11111})) * \log (R^2 P_{10} (1 - P_{S10} P_{S10101}) + 2 R Q P_{11} (1 - P_{S10} P_{S11101}) + (Q^2 P_{DF} P_{10} + Q^2 (1 - P_{DF}) P_{11}) (1 - P_{S11} P_{S11111}))$$

$$- (R^2 P_{10} P_{S10} P_{S10101} + 2 R Q P_{11} P_{S10} P_{S11101} + (Q^2 P_{DF} P_{10} + Q^2 (1 - P_{DF}) P_{11}) P_{S11} P_{S11111}) * \log (R^2 P_{10} P_{S10} P_{S10101} + 2 R Q P_{11} P_{S10} P_{S11101} + (Q^2 P_{DF} P_{10} + Q^2 (1 - P_{DF}) P_{11}) P_{S11} P_{S11111})$$

(Equation 5.65)

$$\mathcal{H}Y2F1^* = - (R^2 P_{00} P_{S00} P_{S00000} + 2 R Q P_{01} P_{S00} P_{S01000} + (Q^2 P_{DF} P_{00} + Q^2 (1 - P_{DF}) P_{01}) P_{S01} P_{S01010}) * \log (R^2 P_{00} P_{S00} P_{S00000} + 2 R Q P_{01} P_{S00} P_{S01000} + (Q^2 P_{DF} P_{00} + Q^2 (1 - P_{DF}) P_{01}) P_{S01} P_{S01010})$$

$$- (R^2 (P_{10} (P_{S00} + P_{S10} P_{S00101}) + P_{00} (P_{S00} P_{S10000} + P_{S10} P_{S00100})) + 2 R Q (P_{11} (P_{S00} + P_{S10} P_{S01101}) + P_{01} (P_{S00} P_{S11000} + P_{S10} P_{S01100})) + (Q^2 P_{DF} P_{10} + Q^2 (1 - P_{DF}) P_{11}) (P_{S01} + P_{S11} P_{S01111})) + (Q^2 P_{DF} P_{00} + Q^2 (1 - P_{DF}) P_{01}) (P_{S01} P_{S11010} + P_{S11} P_{S01110})) * \log (R^2 (P_{10} (P_{S00} + P_{S10} P_{S00101}) + P_{00} (P_{S00} P_{S10000} + P_{S10} P_{S00100})) + 2 R Q (P_{11} (P_{S00} + P_{S10} P_{S01101}) + P_{01} (P_{S00} P_{S11000} + P_{S10} P_{S01100})) + (Q^2 P_{DF} P_{10} + Q^2 (1 - P_{DF}) P_{11}) (P_{S01} + P_{S11} P_{S01111})) + (Q^2 P_{DF} P_{00} + Q^2 (1 - P_{DF}) P_{01}) (P_{S01} P_{S11010} + P_{S11} P_{S01110}))$$

$$- (R^2 (P_{10} P_{S10} P_{S10101} + P_{00} P_{S10} P_{S10100}) + 2 R Q (P_{11} P_{S10} P_{S11101} + P_{01} P_{S10} P_{S11100}) + (Q^2 P_{DF} P_{10} + Q^2 (1 - P_{DF}) P_{11}) P_{S11} P_{S11111} + (Q^2 P_{DF} P_{00} + Q^2 (1 - P_{DF}) P_{01}) P_{S11} P_{S11110}) * \log (R^2 (P_{10} P_{S10} P_{S10101} + P_{00} P_{S10} P_{S10100}) + 2 R Q (P_{11} P_{S10} P_{S11101} + P_{01} P_{S10} P_{S11100}) + (Q^2 P_{DF} P_{10} + Q^2 (1 - P_{DF}) P_{11}) P_{S11} P_{S11111} + (Q^2 P_{DF} P_{00} + Q^2 (1 - P_{DF}) P_{01}) P_{S11} P_{S11110})$$

(Equation 5.66)

$$\mathcal{H}C2F2^* = - R^2 (P_{00} \log P_{00} + P_{10} (1 - P_{S10} P_{S10101}) \log (P_{10} (1 - P_{S10} P_{S10101})) + P_{10} P_{S10} P_{S10101} \log(P_{10} P_{S10} P_{S10101}))$$

$$- 2 R Q (P_{01} \log P_{01} + P_{11} (1 - P_{S10} P_{S11101}) \log(P_{11} (1 - P_{S10} P_{S11101})) + P_{11} P_{S10} P_{S11101} \log (P_{11} P_{S10} P_{S11101}))$$

$$- Q^2 (P_{DF} P_{00} \log P_{DF} P_{00} + (1 - P_{DF}) P_{01} \log ((1 - P_{DF}) P_{01}) + P_{DF} P_{10} (1 - P_{S11} P_{S11111}) \log(P_{DF} P_{10} (1 - P_{S11} P_{S11111})) + (1 - P_{DF}) P_{11} (1 - P_{S11} P_{S11111}) \log((1 - P_{DF}) P_{11} (1 - P_{S11} P_{S11111})) + P_{DF} P_{10} P_{S11} P_{S11111} \log (P_{DF} P_{10} P_{S11} P_{S11111}) + (1 - P_{DF}) P_{11} P_{S11} P_{S11111} \log ((1 - P_{DF}) P_{11} P_{S11} P_{S11111}))$$

(Equation 5.67)

$$\mathcal{H}C2F1^* = - R^2 (P_{00} P_{S00} P_{S00000} \log P_{00} P_{S00} P_{S00000} + (P_{10} (P_{S00} + P_{S10} P_{S00101}) + P_{00} (P_{S00} P_{S10000} + P_{S10} P_{S00100})) * \log (P_{10} (P_{S00} + P_{S10} P_{S00101}) + P_{00} (P_{S00} P_{S10000} + P_{S10} P_{S00100})) + (P_{10} P_{S10} P_{S10101} + P_{00} P_{S10} P_{S10100}) \log(P_{10} P_{S10} P_{S10101} + P_{00} P_{S10} P_{S10100}))$$

$$- 2 R Q (P_{01} P_{S00} P_{S01000} \log P_{01} P_{S00} P_{S01000} + (P_{11} (P_{S00} + P_{S10} P_{S01101}) + P_{01} (P_{S00} P_{S11000} + P_{S10} P_{S01100})) * \log (P_{11} (P_{S00} + P_{S10} P_{S01101}) + P_{01} (P_{S00} P_{S11000} + P_{S10} P_{S01100})) + (P_{11} P_{S10} P_{S11101} + P_{01} P_{S10} P_{S11100}) \log (P_{11} P_{S10} P_{S11101} + P_{01} P_{S10} P_{S11100}))$$

$$- Q^2 ((P_{DF} P_{00} + (1 - P_{DF}) P_{01}) P_{S01} P_{S01010} * \log((P_{DF} P_{00} + (1 - P_{DF}) P_{01}) P_{S01} P_{S01010}) + ((P_{DF} P_{10} + (1 - P_{DF}) P_{11}) * (P_{S01} + P_{S11} P_{S01111}) + (P_{DF} P_{00} + (1 - P_{DF}) P_{01}) * (P_{S01} P_{S11010} + P_{S11} P_{S01110})) * \log((P_{DF} P_{10} + (1 - P_{DF}) P_{11}) * (P_{S01} + P_{S11} P_{S01111}) + (P_{DF} P_{00} + (1 - P_{DF}) P_{01}) * (P_{S01} P_{S11010} + P_{S11} P_{S01110})) + ((P_{DF} P_{10} + (1 - P_{DF}) P_{11}) * P_{S11} P_{S11111} + (P_{DF} P_{00} + (1 - P_{DF}) P_{01}) * P_{S11} P_{S11110}) * \log((P_{DF} P_{10} + (1 - P_{DF}) P_{11}) * P_{S11} P_{S11111} + (P_{DF} P_{00} + (1 - P_{DF}) P_{01}) * P_{S11} P_{S11110}))$$

(Equation 5.68)

$$\mathcal{H}S2F2^* = - P_{S1} \log P_{S1} - P_{S2} \log P_{S2} - P_{S3} \log P_{S3} - P_{S4} \log P_{S4} - P_{S5} \log P_{S5}$$

and

$$\mathcal{H}E2F2^* = P_{S1}\,\mathcal{H}(\varepsilon \mid S1) + P_{S2}\,\mathcal{H}(\varepsilon \mid S2) + P_{S3}\,\mathcal{H}(\varepsilon \mid S3) + P_{S4}\,\mathcal{H}(\varepsilon \mid S4) + P_{S5}\,\mathcal{H}(\varepsilon \mid S5)$$

$$\mathcal{H}E2F2^* = P_{S1} * 0.2 + P_{S2} * 4.85 + P_{S3} * 5.37 + P_{S4} * 0.55 + P_{S5} * 5.54$$

where

$$P_{S1} = R^2 P_{00}\,;\;\; P_{S2} = 2\,R\,Q\,P_{01}\,;\; P_{S3} = Q^2 P_{DF} P_{00} + Q^2 (1 - P_{DF})\, P_{01}\,;$$

$$P_{S4} = R^2 P_{10} + 2\,R\,Q\,P_{11}\,(P_{S00}\,P_{S11001} + P_{S00}\,P_{S01001} / 2 + P_{S10}\,P_{S11101} / 2)\,;$$

$$P_{S5} = (Q^2 - P_{S3}) + 2\,R\,Q\,P_{11}\,(P_{S10}\,P_{S01101} + P_{S00}\,P_{S01001} / 2 + P_{S10}\,P_{S11101} / 2)$$

(Equations 5.69 - 5.75)

$$\mathcal{H}S2F1^* = - P_{S1} \log P_{S1} - P_{S2} \log P_{S2} - P_{S3} \log P_{S3} - P_{S4} \log P_{S4} - P_{S5} \log P_{S5}$$

and

$$\mathcal{H}E2F1^* = P_{S1}\,\mathcal{H}(\varepsilon \mid S1) + P_{S2}\,\mathcal{H}(\varepsilon \mid S2) + P_{S3}\,\mathcal{H}(\varepsilon \mid S3) + P_{S4}\,\mathcal{H}(\varepsilon \mid S4) + P_{S5}\,\mathcal{H}(\varepsilon \mid S5)$$

$$\mathcal{H}E2F1^* = P_{S1} * 0.2 + P_{S2} * 4.85 + P_{S3} * 5.37 + P_{S4} * 0.55 + P_{S5} * 5.54$$

where

$$P_{S1} = R^2 P_{00}\, P_{S00}\, P_{S00000}\,;\;\; P_{S2} = 2\,R\,Q\,P_{01}\, P_{S00}\, P_{S01000}\,;$$

$$P_{S3} = Q^2\,(P_{DF} P_{00} + (1 - P_{DF})\, P_{01})\, P_{S01}\, P_{S01010}\,;$$

$$P_{S4} = (R^2 - P_{S1}) + 2\,R\,Q\,P_{11}\,(P_{S00}\,P_{S11001} + P_{S00}\,P_{S01001} / 2 + P_{S10}\,P_{S11101} / 2) + 2\,R\,Q\,P_{01}\,(P_{S00}\,P_{S11000} + P_{S10}\,P_{S11100} / 2)\,;$$

$$P_{S5} = (Q^2 - P_{S3}) + 2\,R\,Q\,P_{11}\,(P_{S10}\,P_{S01101} + P_{S00}\,P_{S01001} / 2 + P_{S10}\,P_{S11101} / 2) + 2\,R\,Q\,P_{01}\,(P_{S10}\,P_{S01100} + P_{S10}\,P_{S11100} / 2)\,;$$

(Equations 5.76 - 5.82)

Perfect Fault Detection at All Levels

$$\mathcal{H}Y2F2pc = \mathcal{H}Y2F1pc = -R^2 \log R^2 - 2RQ \log 2RQ - Q^2 \log Q^2 = \mathcal{H}S2$$

$$\mathcal{H}C2F2pc = \mathcal{H}C2F1pc = 0; \quad RT2F^*pc = \mathcal{H}S2 \geq RT2pc$$

$$\mathcal{H}S2F2pc = \mathcal{H}S2F1pc = -R^2 \log R^2 - 2RQ \log 2RQ - Q^2 \log Q^2 = \mathcal{H}S2$$

$$\mathcal{H}E2F2pc = \mathcal{H}E2F1pc = R^2 * 0.2 + 2RQ * 0.55 + Q^2 * 5.54 \leq \mathcal{H}E2pc$$

(Equations 5.83 - 5.87)

Worst Fault Detection at All Levels

$$\mathcal{H}Y2F2wc = (2RQ + Q^2) \log (2RQ + Q^2) - R^2 \log R^2 = \mathcal{H}Y2wc$$

$$\mathcal{H}C2F2wc = 0; \quad RT2F2wc = RT2wc$$

$$\mathcal{H}Y2F1wc = -R^2 \log R^2 - 2RQ \log 2RQ - Q^2 \log Q^2 = \mathcal{H}S2$$

$$\mathcal{H}C2F1wc = 0; \quad RT2F1wc = \mathcal{H}S2 = RT2F^*pc$$

$$\mathcal{H}S2F2wc = \mathcal{H}S2F1wc = -R^2 \log R^2 - 2RQ \log 2RQ - Q^2 \log Q^2 = \mathcal{H}S2$$

$$\mathcal{H}E2F2wc = R^2 * 0.55 + 2RQ * 4.85 + Q^2 * 5.37 = \mathcal{H}E2wc$$

$$\mathcal{H}E2F1wc = R^2 * 0.55 + 2RQ * 5.54 + Q^2 * 5.37 \geq \mathcal{H}E2F2wc$$

(Equations 5.88 - 5.96)

Poor Fault Detection at All Levels

$$\mathcal{H}Y2F2poor = \mathcal{H}C2F2poor = -0.5 * \log(0.5) - 0.375 * \log(0.375) - 0.125 * \log(0.125)$$

$$\mathcal{H}Y2F1poor = \mathcal{H}C2F1poor = -0.125 * \log(0.125) - 0.625 * \log(0.625) - 0.25 * \log(0.25)$$

$$\mathcal{H}C2F2poor = 0.974 > \mathcal{H}C2F1poor = 0.900; \quad RT2F*poor = \mathbf{0}$$

$$\mathcal{H}E2F2poor = R^2 * 0.1 + R\,Q * 4.85 + Q^2 * 2.685 + (R^2 + R\,Q) * 0.275 + (Q^2 + R\,Q) * 2.77 = \mathcal{H}E2poor \geq \mathcal{H}E1$$

$$\mathcal{H}E2F1poor = R^2 * 0.025 + R\,Q * 1.213 + Q^2 * 0.671 + (R^2 + R\,Q) * 0.481 + (Q^2 + R\,Q) * 4.85 \approx \mathcal{H}E2poor$$

(Equations 5.97 - 5.102)

Perfect Duplex and Poor Simplex Fault Detection

$$\mathcal{H}Y2F2pc,poor = -R^2 \log R^2 - (2\,R\,Q + Q^2) * (0.75) \log((2\,R\,Q + Q^2) * (0.75)) - (2\,R\,Q + Q^2) * (0.25) \log((2\,R\,Q + Q^2) * (0.25))$$

$$\mathcal{H}C2F2pc,poor = -(2\,R\,Q + Q^2) * (0.75 * \log(0.75) + 0.25 * \log(0.25))$$

$$\mathcal{H}Y2F1pc,poor = -R^2 * 0.5 * (\log(R^2 * 0.5) + \log(R^2 * 0.25)) - (2\,R\,Q + Q^2) * (0.75) \log((2\,R\,Q + Q^2) * (0.75)) - (2\,R\,Q + Q^2) * (0.25) \log((2\,R\,Q + Q^2) * (0.25))$$

$$\mathcal{H}C2F1pc,poor = -R^2 * 0.5 * (\log(0.5) + \log(0.25)) - (2\,R\,Q + Q^2) * (0.75 * \log(0.75) + 0.25 * \log(0.25))$$

$$\mathcal{H}C2F2pc,poor > \mathcal{H}C2F1pc,poor; \quad RT2F*pc,poor = RT2pc = \mathcal{H}Y2pc$$

$$\mathcal{H}E2F2pc,poor = R^2 * 0.2 + R\,Q * 0.55 + (Q^2 + R\,Q) * 5.54 = \mathcal{H}E2pc$$

$$\mathcal{H}E2F1pc,poor = R^2 * 0.05 + (R^2 * 0.75 + R\,Q) * 0.55 + (Q^2 + R\,Q) * 5.54 \approx \mathcal{H}E1 \approx \mathcal{H}E2pc$$

(Equations 5.103 - 5.110)

Poor Duplex and Perfect Simplex Fault Detection

$$\mathcal{H}Y2F2poor,pc = - 0.5 \log 0.5 - (2 R Q + R^2) * (0.5) * \log ((2 R Q + R^2) * (0.5)) - Q^2 * (0.5) * \log (Q^2 * 0.5)$$

$$\mathcal{H}C2F2poor,pc = - \log 0.5 = \log 2$$

$$RT2F2poor,pc = - (1 - Q^2) * (0.5) * \log (1 - Q^2) - Q^2 * (0.5) * \log Q^2 \leq 0.5 * \log 2$$

$$\mathcal{H}Y2F1poor,pc = - R^2 * 0.5 * \log (R^2 * 0.5) - (2 R Q + R^2 * 0.5) * \log (2 R Q + R^2 * 0.5) - Q^2 \log Q^2$$

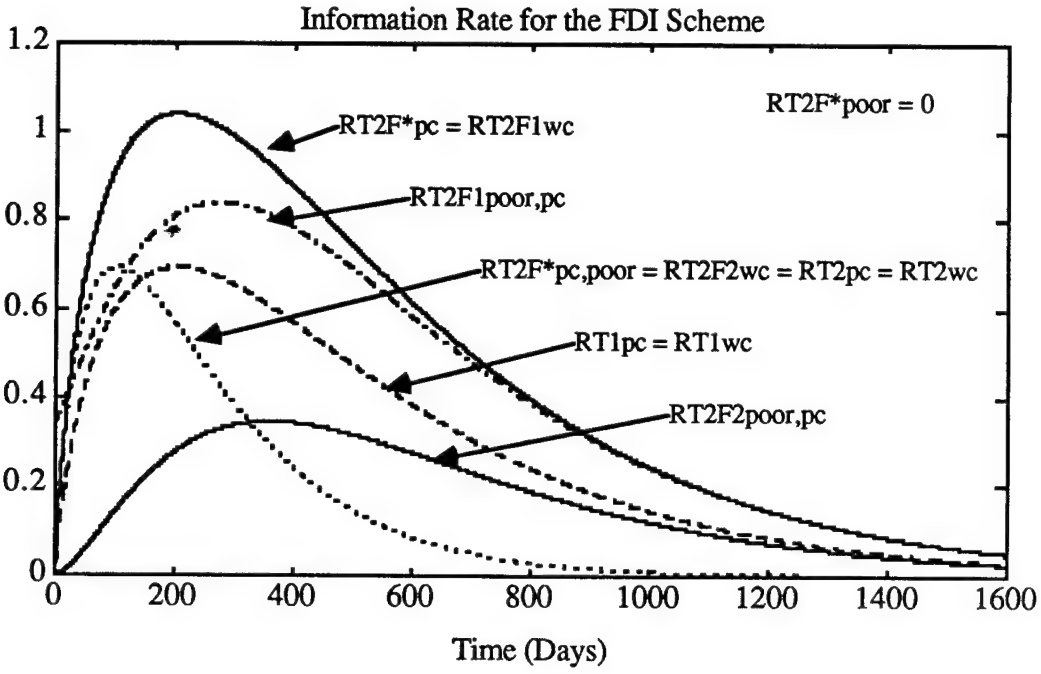
$$\mathcal{H}C2F1poor,pc = - R^2 \log 0.5 \leq \mathcal{H}C2F2poor,pc$$

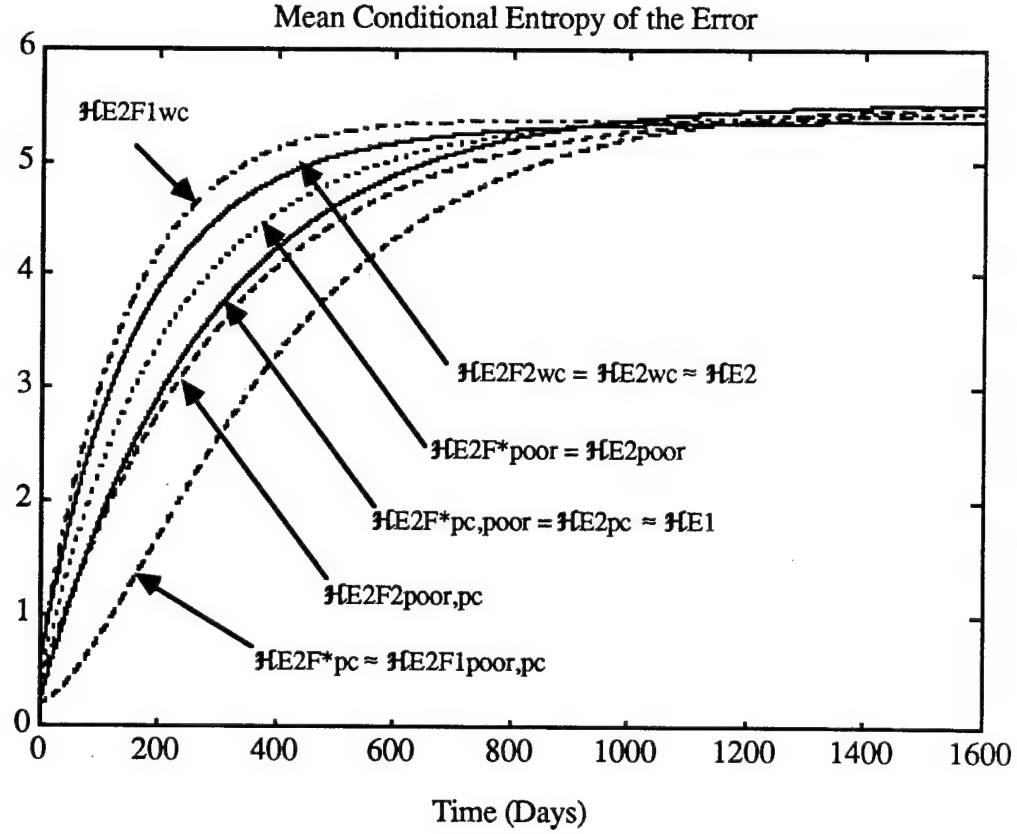
$$RT2F1poor,pc = - R^2 * 0.5 * \log R^2 - (2 R Q + R^2 * 0.5) * \log (2 R Q + R^2 * 0.5) - Q^2 \log Q^2$$

$$\mathcal{H}E2F2poor,pc = R^2 * 0.1 + R Q * 4.85 + Q^2 * 2.685 + (R^2 + 2 R Q) * 0.275 + Q^2 * 2.77$$

$$\mathcal{H}E2F1poor,pc = R^2 * 0.1 + (R^2 * 0.5 + 2 R Q) * 0.55 + Q^2 * 5.54 \approx \mathcal{H}E2F*pc$$

(Equations 5.111 - 5.118)





Figures 5.18, 5.19

Duplex FDI alone provides the same results for a dual structure as full FDI which incorporates a poor simplex test (i.e. RT2* = RT2F2* and $\mathcal{H}$E2* = $\mathcal{H}$E2F2*). These results are improved upon by any full FDI scheme with a better simplex test. Hence, a dual structure with full FDI allows equivalent or better performance than with duplex FDI alone.

In all cases of importance, full FDI with simplex precedence (RT2F1*, $\mathcal{H}$E2F1*) for conflict resolution provides better performance than the case of duplex precedence (RT2F2*, $\mathcal{H}$E2F2*). As observed in Figure 5.18, duplex precedence can be costly in terms of information transfer (e.g. RT2F2poor,pc < RT2F1poor,pc). Even in cases of equivalent information rates (e.g. Equations 5.99, 5.107, and 5.115), duplex precedence exhibits a larger loss of information due to decision error ($\mathcal{H}$C2F2* > $\mathcal{H}$C2F1*). In Figure 5.19, it is observed that duplex precedence allows a greater error variance than simplex precedence ($\mathcal{H}$E2F2* ≥ $\mathcal{H}$E2F1*). Hence, simplex precedence must be utilized by a dual structure with full FDI and without shutdown capability.

The perfect case of errorless detection for a dual structure with full FDI exhibits a dramatic improvement over single structure performance in terms of reduced error variance due to the second-order effect of its fault tolerance. Single structure performance is defined by $\mathcal{H}$E1 irregardless of any simplex tests. Error variance for a perfect dual structure is initially lower due to the averaging of two working controllers and is only gradually increased upon switching to the second stage of a single working controller (Figure 5.19). Perfect and worst case fault detection for a dual structure with full FDI are found to provide the highest rate of information transmission, while poor or noisy fault detection has a zero transmission rate (Figure 5.18). The general improvement of a dual structure over the performance of a single structure is dictated by the quality of the simplex test (Figure 5.20). This is because the cost of missed detection can be offset by giving precedence to the simplex test and the cost of a false alarm is small for a structure without shutdown

capability. Hence, a dual structure without shutdown capability can achieve slightly better performance than a single structure with a poor simplex test and significantly better performance with a fair or better simplex test.

Full Dual Structure		
Duplex Test	Simplex Test	Performance Comparison
any	worst	$\mathcal{H}$E1 ≤ $\mathcal{H}$E2F#*poor ≤ $\mathcal{H}$E2F#*wc
any	poor	$\mathcal{H}$E1 ≤ $\mathcal{H}$E2F#*poor
poor or better	fair	$\mathcal{H}$E2F#*fair ≤ $\mathcal{H}$E1
poor or better	perfect	$\mathcal{H}$E2F#*pc ≤ $\mathcal{H}$E2F#*fair ≤ $\mathcal{H}$E1

Figure 5.20 Comparison of Full Dual Structure and Single Structure

The relative merit of a fault detection scheme for a dual control structure is now examined where system shutdown is a possible system state. Here, the system state of false alarm is given the same weight as missed detection in the tabulation of entropy for the error function (as in Figure 5.11). System shutdown is initiated immediately upon detection of a fault which cannot be isolated. Here, the benefit of a fault detection scheme is to avoid faulty performance or product by simply ending the mission.

$$\mathcal{H}E2F2^* = P_{S1}\,\mathcal{H}(\varepsilon \mid S1) + P_{S2}\,\mathcal{H}(\varepsilon \mid S2) + P_{S3}\,\mathcal{H}(\varepsilon \mid S3) + P_{S4}\,\mathcal{H}(\varepsilon \mid S4) + P_{S5}\,\mathcal{H}(\varepsilon \mid S5) + P_{FS}\,\mathcal{H}(\varepsilon \mid \text{False Shutdown}) + P_{SD}\,\mathcal{H}(\varepsilon \mid \text{Shutdown})$$

$$\mathcal{H}E2F2^* = P_{S1} * 0.2 + P_{S2} * 4.85 + P_{S3} * 5.37 + P_{S4} * 0.55 + (P_{S5} + P_{FS}) * 5.54$$

where

$$P_{S1} = R^2\,P_{00};\quad P_{S2} = 2\,R\,Q\,P_{01};\quad P_{S3} = Q^2\,P_{DF}\,P_{00} + Q^2\,(1 - P_{DF})\,P_{01};$$

$$P_{S4} = R^2\,P_{10}\,(1 - P_{S10}\,P_{S10101}) + 2\,R\,Q\,P_{11}\,(P_{S00}\,P_{S11001} + P_{S00}\,P_{S01001} / 2);$$

$$P_{FS} = R^2\,P_{10}\,P_{S10}\,P_{S10101} + 2\,R\,Q\,P_{11}\,P_{S10}\,P_{S11101};$$

$$P_{S5} = 2\,R\,Q\,P_{11}\,(P_{S10}\,P_{S01101} + P_{S00}\,P_{S01001} / 2) + Q^2\,(P_{DF}\,P_{10} + (1 - P_{DF})\,P_{11})\,(P_{S01} + P_{S11}\,P_{S01111});$$

$$P_{SD} = Q^2\,(P_{DF}\,P_{10} + (1 - P_{DF})\,P_{11})\,P_{S11}\,P_{S11111}$$

(Equations 5.119 - 5.126)

$$\mathcal{H}E2F1^* = P_{S1}\,\mathcal{H}(\varepsilon \mid S1) + P_{S2}\,\mathcal{H}(\varepsilon \mid S2) + P_{S3}\,\mathcal{H}(\varepsilon \mid S3) + P_{S4}\,\mathcal{H}(\varepsilon \mid S4) + P_{S5}\,\mathcal{H}(\varepsilon \mid S5) + P_{FS}\,\mathcal{H}(\varepsilon \mid \text{False Shutdown}) + P_{SD}\,\mathcal{H}(\varepsilon \mid \text{Shutdown})$$

$$\mathcal{H}E2F1^* = P_{S1} * 0.2 + P_{S2} * 4.85 + P_{S3} * 5.37 + P_{S4} * 0.55 + (P_{S5} + P_{FS}) * 5.54$$

where

$$P_{S1} = R^2\,P_{00}\,P_{S00}\,P_{S00000};\quad P_{S2} = 2\,R\,Q\,P_{01}\,P_{S00}\,P_{S01000};$$

$$P_{S3} = Q^2\,(P_{DF}\,P_{00} + (1 - P_{DF})\,P_{01})\,P_{S01}\,P_{S01010};$$

$$P_{S4} = R^2\,(P_{10}\,(P_{S00} + P_{S10}\,P_{S00101}) + P_{00}\,(P_{S00}\,P_{S10000} + P_{S10}\,P_{S00100})) + 2\,R\,Q\,P_{11}\,(P_{S00}\,P_{S11001} + P_{S00}\,P_{S01001} / 2) + 2\,R\,Q\,P_{01}\,P_{S00}\,P_{S11000};$$

$$P_{FS} = R^2\,(P_{00}\,P_{S10}\,P_{S10100} + P_{10}\,P_{S10}\,P_{S10101}) + 2\,R\,Q\,(P_{01}\,P_{S10}\,P_{S11100} + P_{11}\,P_{S10}\,P_{S11101});$$

$$P_{S5} = (Q^2 - P_{S3} - P_{SD}) + 2\,R\,Q\,P_{11}\,(P_{S10}\,P_{S01101} + P_{S00}\,P_{S01001} / 2) + 2\,R\,Q\,P_{01}\,P_{S10}\,P_{S01100};$$

$$P_{SD} = Q^2\,(P_{DF}\,P_{10} + (1 - P_{DF})\,P_{11})\,P_{S11}\,P_{S11111} + Q^2\,(P_{DF}\,P_{00} + (1 - P_{DF})\,P_{01})\,P_{S11}\,P_{S11110}$$

(Equations 5.127 - 5.134)

Perfect Detection: $\mathcal{H}E2F^*pc = R^2 * 0.2 + 2\,R\,Q * 0.55$ (Equations 5.135)

Worst Fault Detection at All Levels

$$\mathcal{H}E2F2wc = R^2 * 5.54 + 2\,R\,Q * 4.85 + Q^2 * 5.37 \leq \mathcal{H}E1wc$$

$$\mathcal{H}E2F1wc = (R^2 + 2\,R\,Q) * 5.54 + Q^2 * 5.37 \leq \mathcal{H}E1wc$$

(Equations 5.136, 5.137)

Poor Fault Detection at All Levels

$$\mathcal{H}E2F2poor = R^2 * 0.1 + R\,Q * 4.85 + Q^2 * 2.685 + (R^2 + R\,Q) * 0.206 + (R^2 + 5\,R\,Q + 3\,Q^2) * 0.693 \leq \mathcal{H}E1poor$$

$$\mathcal{H}E2F1poor = R^2 * 0.025 + R\,Q * 1.213 + Q^2 * 0.671 + (R^2 + R\,Q) * 0.344 + (2\,R^2 + 9\,R\,Q + 5\,Q^2) * 0.693 \approx \mathcal{H}E2F2poor$$

(Equations 5.138, 5.139)

Perfect Duplex and Poor Simplex Fault Detection

$$\mathcal{H}E2F2pc,poor = R^2 * 0.2 + R\,Q * 0.413 + (5\,R\,Q + 3\,Q^2) * 1.39$$

$$\mathcal{H}E2F1pc,poor = R^2 * 0.05 + (2\,R^2 + 3\,R\,Q) * 0.138 + (R^2 + 5\,R\,Q + 3\,Q^2) * 1.39$$

(Equations 5.140, 5.141)

Poor Duplex and Perfect Simplex Fault Detection

$$\mathcal{H}E2F2poor,pc = R^2 * 0.1 + R\,Q * 4.85 + Q^2 * 2.685 + (R^2 + 2\,R\,Q) * 0.275$$

$$\mathcal{H}E2F1poor,pc = R^2 * 0.1 + (R^2 * 0.5 + 2\,R\,Q) * 0.55 \approx \mathcal{H}E2F^*pc$$

(Equations 5.142, 5.143)

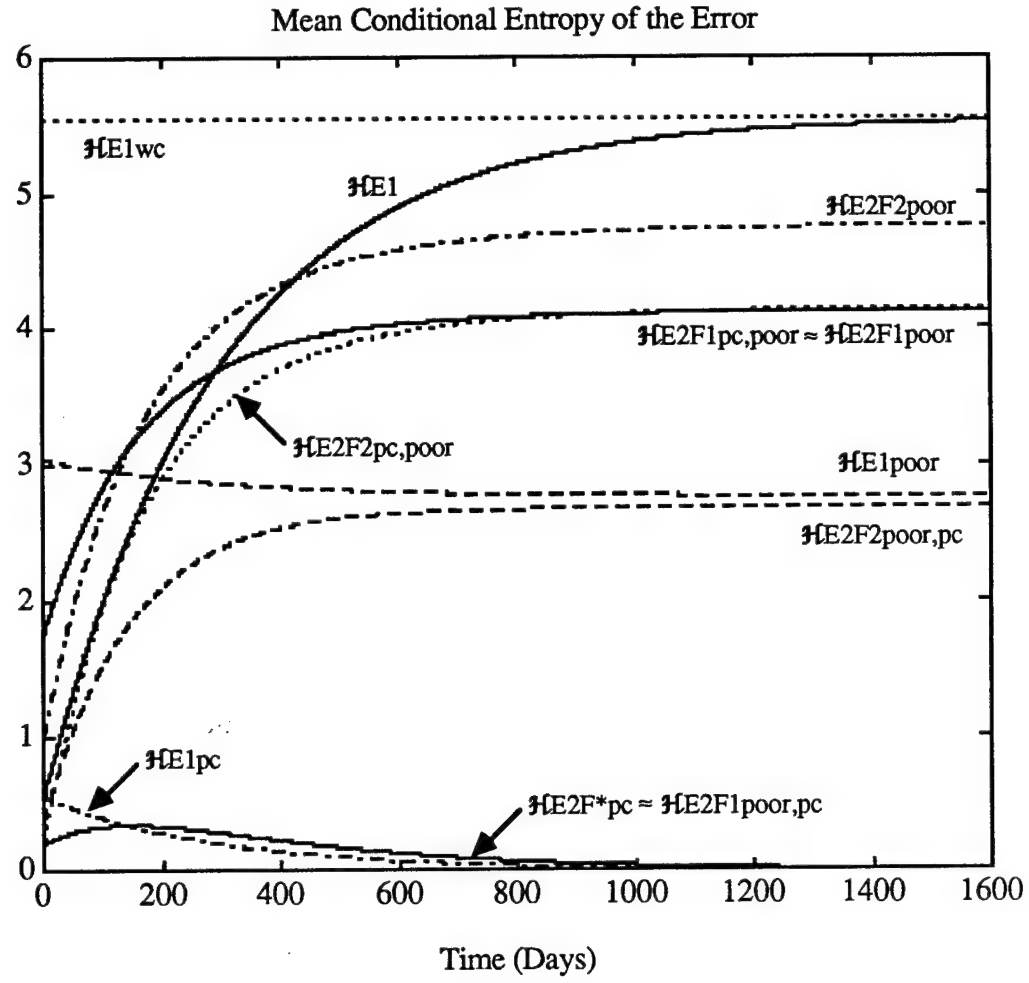
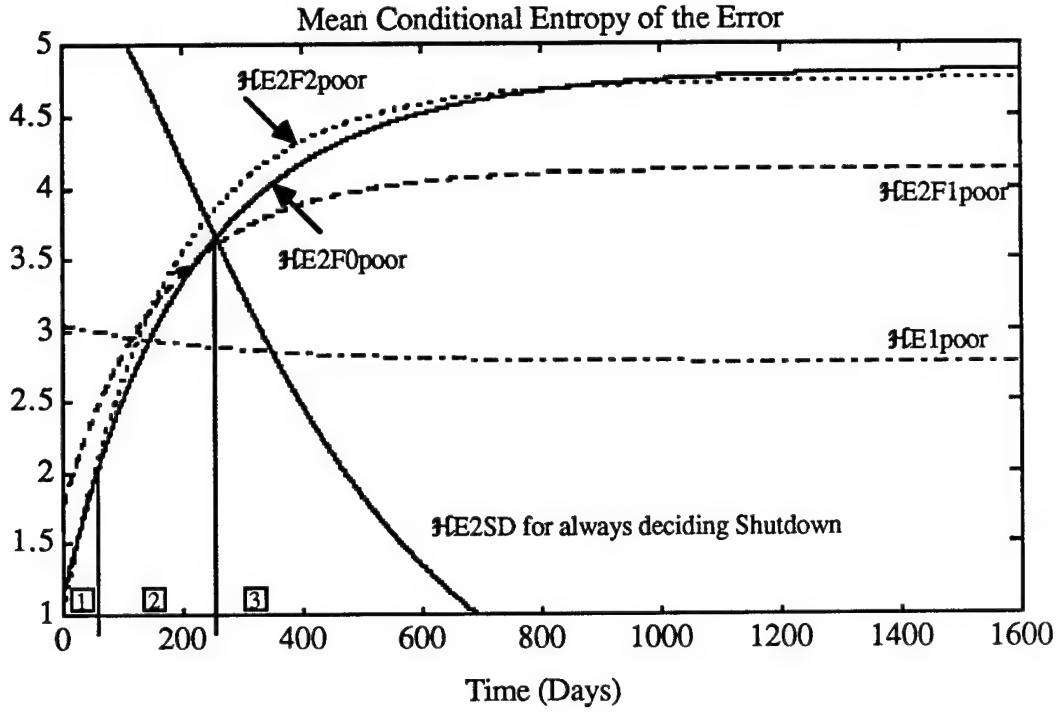
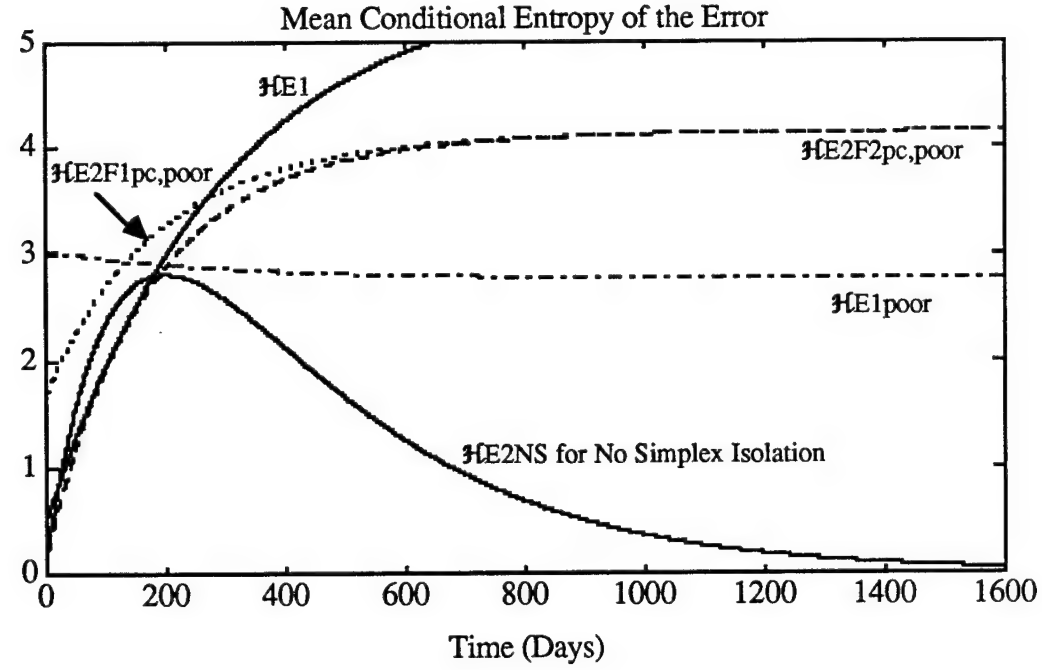


Figure 5.21 Error Entropy for Dual Structure with Shutdown and False Alarm Cost



Figures 5.22 Mission Stages for Different FDI Schemes



Figures 5.23 Improvement by Ignoring Poor Simplex Tests

Results indicate the need to switch the FDI decision scheme for different stages of the mission in all but the most perfect case. A dual structure with full FDI can achieve better average performance with duplex precedence (assume both working unless difference test fails) in early stages of the mission where R^2 = pr{Both Working} dominates and with simplex precedence (assume dual or single fault unless all tests pass) in the later stages of the mission where Q^2 = pr{Both Failed} dominates. A third decision scheme with no precedence (assume single fault unless all tests agree otherwise) suggests a middle stage for the full FDI scheme when 2RQ = pr{Single Fault} dominates. It is concluded that precedence for the full FDI scheme should agree with the most probable state for the given mission time (i.e. assume the dominant prior when designing the decision scheme). Figure 5.22 illustrates this concept of a staged FDI scheme for the case of poor fault detection at all levels. A fourth decision scheme, where no FDI is employed and shutdown is always decided, is suggested by Figure 5.22 as a better alternative for the third stage of a poor detection scheme due to its lower error entropy ($\mathcal{H}$E2SD).

If either level of tests (duplex or simplex) should dominate the other in quality, then the switching times for the mission stages must be adjusted accordingly. For example, as the quality of the duplex test approaches the perfect case, switching times will be pushed further and further out until finally duplex precedence (i.e. $\mathcal{H}$E2F2pc,poor) will be utilized throughout the mission. The same holds for the simplex test (i.e. $\mathcal{H}$E2F1poor,pc has a lower error variance than $\mathcal{H}$E2F2poor,pc over the entire mission).

The perfect case of errorless detection for a dual structure with full FDI exhibits a dramatic improvement over single structure performance in terms of a longer average mission before shutdown. Also, error variance for any dual structure is initially lower than for a single structure due to the averaging of two working controllers. The general improvement of a dual structure over the performance of a single structure is dictated by the quality of both tests. For example, a dual structure with poor FDI at both levels reaches an error variance much higher than that for a single structure (Figure 5.22). This difference can be offset by deciding shutdown for the third stage of the decision scheme ($\mathfrak{H}$E2SD). The increased error variance during the second stage cannot be further reduced due to the inability to isolate the first failure by the poor simplex test. However, a dual structure with a poor simplex test and a perfect duplex test can achieve lower error entropy than a single structure with the same poor simplex test over the entire mission (Figure 5.23, $\mathfrak{H}$E2F2pc,poor & $\mathfrak{H}$E2NS < $\mathfrak{H}$E1 & $\mathfrak{H}$E1poor). This is made possible by a second and final decision stage where only the perfect duplex test is utilized and shutdown is initiated upon a failed difference test ($\mathfrak{H}$E2NS). Good results can also be obtained with a perfect simplex test and a poor duplex test (i.e. $\mathfrak{H}$E2F1poor,pc < $\mathfrak{H}$E1pc). Hence, full FDI for a dual structure with shutdown capability must incorporate a near-perfect test at one or both levels in order to improve upon single structure performance.

5.6.4. Entropy Analysis of Triple Redundant Structures

In this section, the relative merit of a fault detection scheme for a triple redundant control structure is examined. Results follow those of the previous section. In the exercises of this thesis, it has been assumed that system shutdown is not a possible system state. Hence, no matter what decision branch is followed by a fault detection scheme, at least one control structure will be utilized in the estimates of the controlled parameter for the length of the mission. The benefit of a fault detection scheme in this situation is to alert the operator and to isolate any possible failure so that continuous operation can be maintained with the working controller. Two fault detection schemes of differing performance are examined with respect to entropy and information transmission: the Triple Redundant Structure (TRS) detailed in Chapter 4 with perfect triplex detection and poor simplex detection, and the perfect case of errorless detection at all levels. The failure rate of the example reliability budget (0.000142, Figure 3.7) and the conditional error entropies of Figure 5.5 are used in producing the following figures. In each case, the following are derived and compared:

1) Outcome entropy $\mathcal{H}Y3^*$, mean conditional entropy $\mathcal{H}C3^*$, and rate of information transmission $RT3^* = \mathcal{H}Y3^* - \mathcal{H}C3^*$ for the FDI channel or decision.

2) System state entropy $\mathcal{H}S3^*$, mean conditional entropy of the estimation error $\mathcal{H}E3^*$, and system or joint entropy $\mathcal{H}3^* = \mathcal{H}S3^* + \mathcal{H}E3^*$.

A control structure with a decision scheme of maximum rate and minimum error variance is optimal with respect to entropy (Section 5.5. and 5.5.1). The estimation error entropy for these full FDI schemes will be compared with those of two techniques for passive redundancy: majority voting and fault masking.

Note: * represents a suffix (e.g. pc, wc, poor) used to distinguish the results for different FDI schemes. Results for a redundant structure with a passive technique will be distinguished here (e.g. V for majority voting and M for fault masking).

Perfect Fault Detection at All Levels

$$RT3pc = -R^3 \log R^3 - 3QR^2 \log 3QR^2 - 3RQ^2 \log 3RQ^2 - Q^3 \log Q^3 = \mathcal{H}S3$$

$$\mathcal{H}E3pc = 3QR^2 * 0.2 + 3RQ^2 * 0.55 + Q^3 * 5.54 \leq \mathcal{H}E2F*pc \leq \mathcal{H}E1$$

(Equations 5.144, 5.145)

TRS (Perfect Triplex and Duplex and Poor Simplex) Fault Detection

$$\mathcal{H}Y3pc,poor = -R^3 \log R^3 - 3QR^2 \log 3QR^2 - (3RQ^2 + Q^3) * (0.75) \log ((3RQ^2 + Q^3) * (0.75)) - (3RQ^2 + Q^3) * (0.25) \log ((3RQ^2 + Q^3) * (0.25))$$

$$\mathcal{H}C3pc,poor = -(3RQ^2 + Q^3) * (0.75 * \log (0.75) + 0.25 * \log(0.25))$$

$$RT3pc,poor = -R^3 \log R^3 - 3QR^2 \log 3QR^2 - (3RQ^2 + Q^3) \log (3RQ^2 + Q^3)$$

$$\mathcal{H}E3pc,poor = 3QR^2 * 0.2 + RQ^2 * 0.55 + (2RQ^2 + Q^3) * 5.54$$

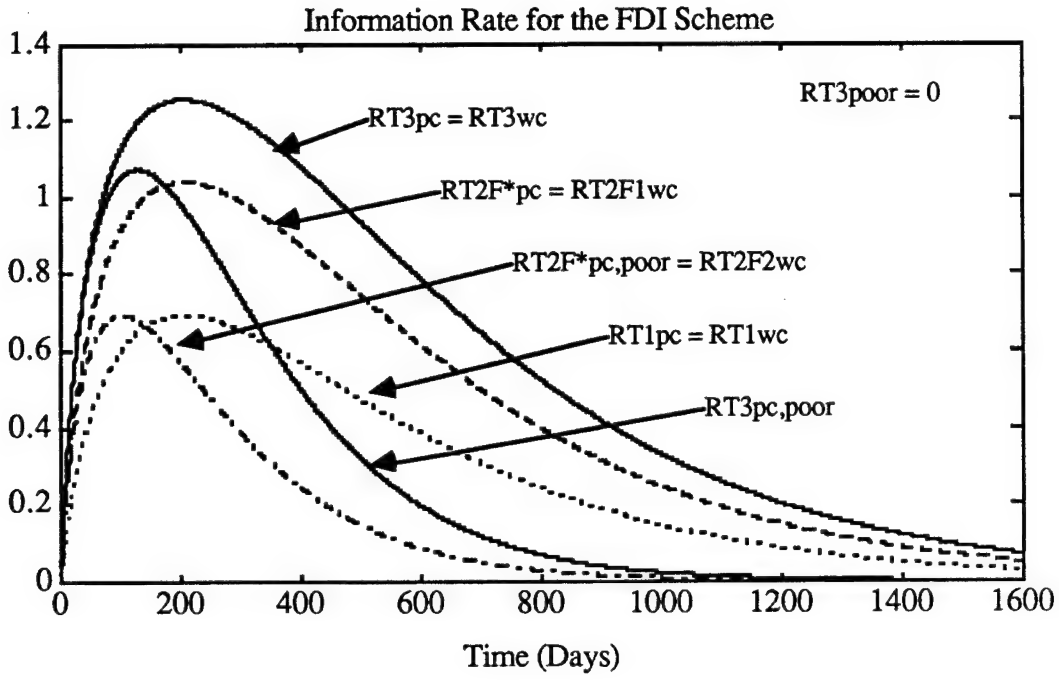
(Equations 5.146 - 5.149)

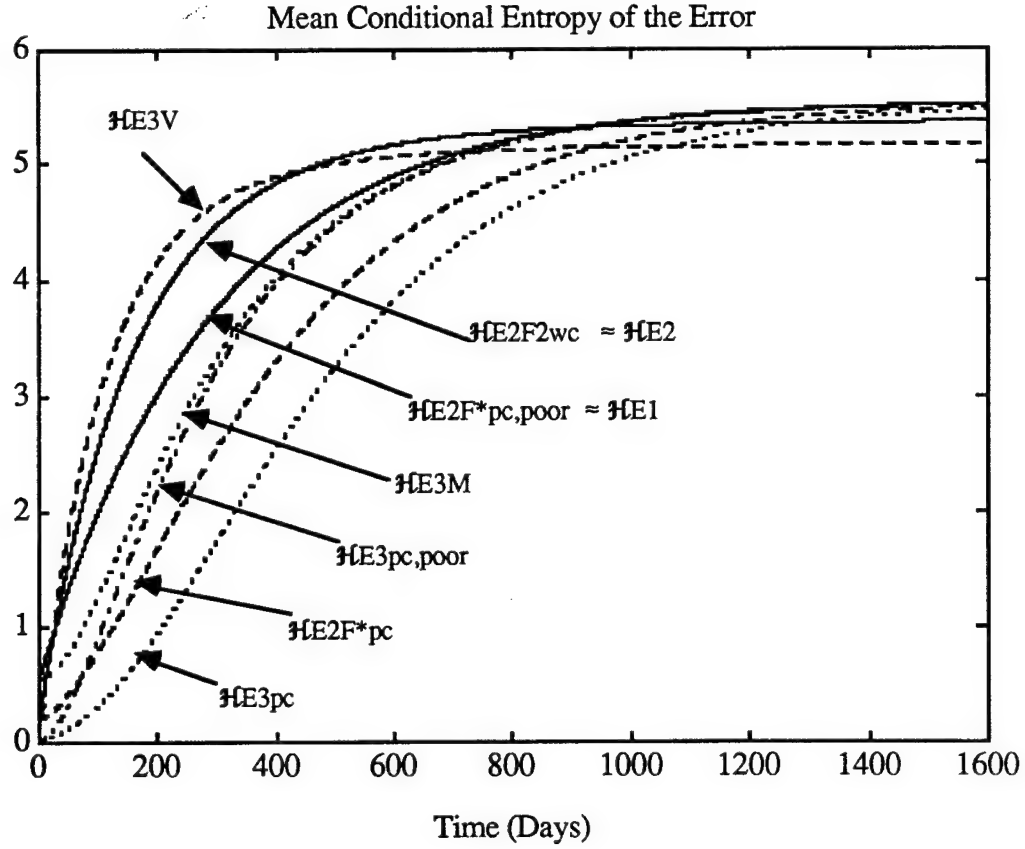
Passive Redundancy Techniques: Fault Masking and Majority-Voting

$$\mathcal{H}E3M = (R^3 + 3QR^2 + RQ^2) * 0.55 + (2RQ^2 + Q^3) * 5.54 \geq \mathcal{H}E3pc,poor$$

$$\mathcal{H}E3V = 3QR^2 * 4.45 + 3RQ^2 * 4.97 + Q^3 * 5.17$$

(Equations 5.150, 5.151)





Figures 5.24, 5.25

Perfect and worst case fault detection for a triple structure with full FDI are found to provide the highest rate of information transmission, while poor or noisy fault detection has a zero transmission rate (Figure 5.24). The perfect case of errorless detection for a triple structure with full FDI exhibits a dramatic improvement over single and dual structure performance in terms of reduced error variance due to the third-order effect of its fault tolerance. Single structure performance is defined by $\mathfrak{H}E1$ irregardless of any simplex tests. Error variance for any redundant structure is initially lower due to the averaging of working controllers and is only gradually increased upon switching to successive stages of reduced operation (Figure 5.25). The relative improvement of the dual structure over the single structure is dependent upon the quality of the simplex test. However, a triple redundant structure of near-perfect triplex and duplex detection and poor simplex detection shows immediate improvement over single structure performance. It also found to provide lower error entropy than both of the examined passive redundancy techniques, although it does approach the performance of a fault masking scheme as the mission progresses. Fault masking shows similar promise while majority-voting is easily observed as undesirable. Hence, a triple structure without shutdown capability can achieve significantly better performance than a single or dual structure.

The relative merit of a fault detection scheme for a triple control structure is now examined where system shutdown is a possible system state. Here, the system state of false alarm is given the same weight as missed detection in the tabulation of entropy for the error function (as in Figure 5.11). Here, the benefit of a fault detection scheme is to avoid faulty performance or product by simply ending the mission.

Perfect Fault Detection at All Levels

$$\mathcal{H}E3pc = 3\,Q\,R^2 * 0.2 + 3\,R\,Q^2 * 0.55 \leq \mathcal{H}E2F*pc \leq \mathcal{H}E1 \qquad \text{(Equation 5.152)}$$

TRS (Perfect Triplex and Duplex and Poor Simplex) Fault Detection

$$\mathcal{H}E3pc,poor = 3\,Q\,R^2 * 0.2 + R\,Q^2 * 0.413 + (9\,R\,Q^2 + 3\,Q^3) * 1.39$$

(Equation 5.153)

Perfect Triplex and Duplex and No Simplex Fault Detection

$$\mathcal{H}E3NS = 3\,Q\,R^2 * 0.2 + 3\,R\,Q^2 * 5.54 \qquad \text{(Equation 5.154)}$$

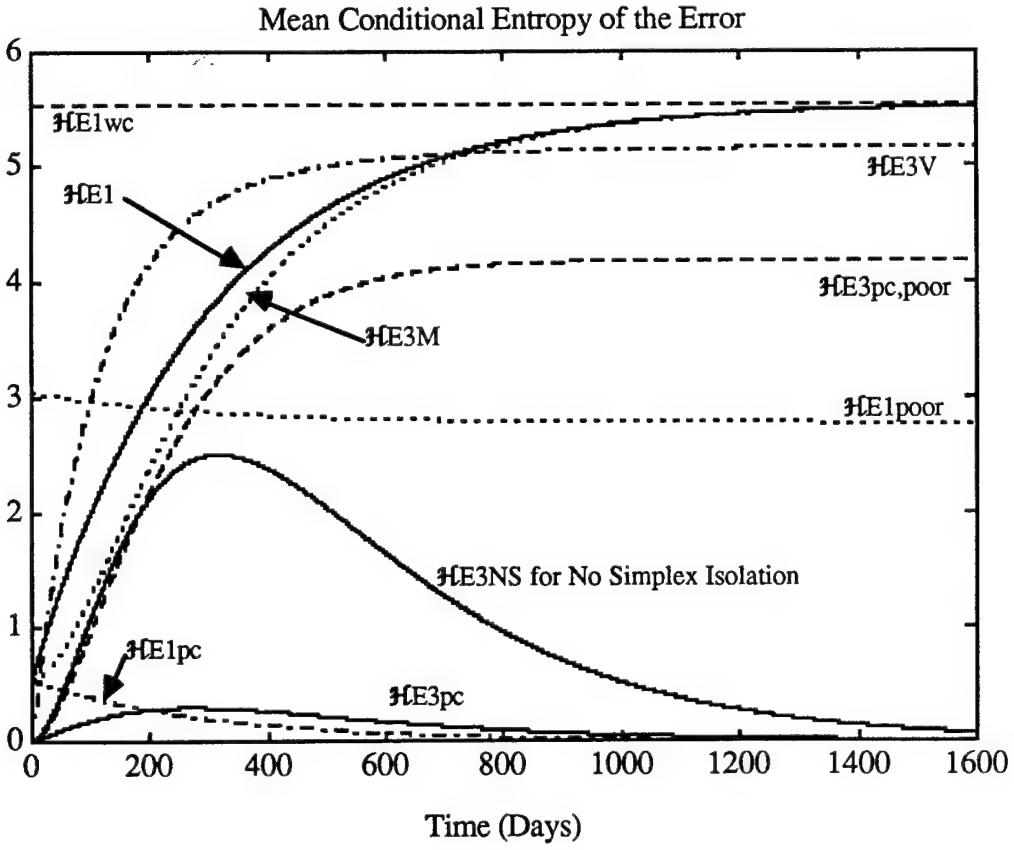


Figure 5.26 Error Entropy for Triple Structure with Shutdown and False Alarm Cost

The perfect case of errorless detection for a triple structure with full FDI exhibits a dramatic improvement over single structure performance in terms of a longer average mission before shutdown (i.e. the mission time where $\mathcal{H}$E3pc = 0). Also, error variance for any redundant structure is initially lower than for a single structure due to the averaging of working controllers. The general performance of a triple structure with shutdown is dependent upon the quality of the tests and proper design of the decision scheme (Figure 5.26). For example, a triple structure with a poor simplex test (e.g. the TRS) reaches an error variance much higher than that for a single structure. A second and final decision stage, where the poor simplex test is not utilized and shutdown is initiated upon a failed difference test, can achieve lower error entropy than either a single or dual structure over the entire mission ($\mathcal{H}$E3pc,poor & $\mathcal{H}$E3NS < $\mathcal{H}$E2F2pc,poor & $\mathcal{H}$E2NS < $\mathcal{H}$E1 & $\mathcal{H}$E1poor). Good results can also be obtained with a perfect simplex test and a poor duplex test. Hence, full FDI for a triple structure with shutdown capability must incorporate a near-perfect test in order to improve upon single structure performance. The passive redundancy techniques of fault masking and majority-voting are obviously not meant for a system with shutdown capability.

5.7. Conclusion

In this chapter, we seek to analyze all relevant a priori uncertainty or entropy within the control system. The minimized Gaussian error function and the maximized exponential reliability function provide a complete concept of all a priori knowledge of the control structure. The marginal or conditional probabilities of the FDI schemes describe the performance statistics associated with the redundant structure. The resultant set of system states and their associated probabilities, as illustrated by the decision tree, represents all a priori uncertainty in the control system.

Information theory defines entropy as a logarithmic measure of the randomness or 'choice' involved in an event or the prior uncertainty of the outcome of an experiment. Entropy can be formulated from the probabilities of an exhaustive set of n possible events or states (discrete case) or from the probability density function of a continuous distribution (continuous case). The concept of entropy has a rich history that defies disciplinary boundaries in its application. Its widespread application attests to its fundamental nature and allows for linkage into a more comprehensive system representation of uncertainty by incorporation of other system entropies. Thus, entropy is a measure of our a priori knowledge or, more appropriately, lack of knowledge (i.e. ignorance/uncertainty) in terms of the a priori probabilities. Further, this metric of uncertainty allows for comparisons of the effective system performance for different redundant structures.

Shannon evaluated the performance of a general communication system in the presence of noise. In this context, a control structure can be considered the channel which attempts to communicate control needs to the process while contending with error or noise sources inherent within the signal transmission. Due to these errors, it is not possible to completely reconstruct the transmitted signal by any operation upon the received signal and

information is lost. A system designer always tries to optimize the rate of transmission by maximizing source information and by minimizing information losses due to interference. A large bandwidth and signal-to-noise ratio (SNR) is desired for the source and a minimized variance is desired for the Gaussian noise or error in order to maximize the information rate of the control structure.

Shannon found methods of transmitting or encoding the source signal which are optimal in combating noise. By Shannon's Fundamental Theorem, if the entropy or information of a source is less than the system's capacity, then there exists an encoding scheme for transmission across the channel which achieves an arbitrarily small probability of error. This is possible by sending the information in a redundant form and performing a statistical analysis on the different received versions of the message. This reduction in decision error causes a subsequent reduction in the lost information due to noise and, hence, an increase in the rate of transmission for the channel. However, these benefits are at a cost of increased complexity and either: hardware for physical redundancy, or delay for repeated messages over the same channel. The cost of errorless transmission is infinite communication channels or infinite delay time. Hence, it is not possible to transmit information over a noisy channel without some probability of error.

A redundant structure can be considered the channel which attempts to correctly determine or communicate the current state of the system while contending with error or noise sources inherent within the decision. The system states and error sources possible for a redundant structure can be identified by a decision tree. This decision tree also represents explicitly the discrete communication or information channel for a redundant structure. Due to decision errors in the FDI scheme, it is not possible to completely know the current system state by any operation upon the parity vector and information can be lost.

The rate of information transmission across the discrete channel of the FDI decision scheme is optimized by maximizing the mutual information between the input and output states. First, the extent of our a priori or input knowledge $\mathfrak{H}(X)$ is maximized. The entropy of the exponential reliability distribution is defined by the MTBF. Hence, a more reliable control structure with a greater MTBF is desired. Second, system or output knowledge $\mathfrak{H}(Y)$ is maximized by increasing the granularity or number of the output system states. Entropy of the system state set exhibits a characteristic "humped" curve which monotonically increases with the level of redundancy. However, the gains of this additional knowledge cannot be realized (and can even be at a detriment) if it is accompanied by poor utilization or transmission losses. The channel loss or uncertainty of the FDI scheme must be minimized by approaching the ideal, matched transmission scheme. Proper utilization of a redundant structure would also minimize the error variance of the controlled parameter. This corresponds with the perfect-case of errorless decision. A large failure signal-to-noise ratio (SNR) is required in order to approach the perfect-case. The mean conditional entropy of the error or noise is found to decrease with each level of redundancy when a near-optimal FDI scheme is employed. In conclusion, the optimal rate of information transmission for the discrete FDI decision scheme of a redundant structure for fault-tolerance is reached by utilizing a highly reliable control structure at the greatest level of redundancy while maintaining near-perfect FDI at all levels of operation. This allows maximizing the information rate of the FDI decision scheme while minimizing the error variance of the controlled parameter. Further, the average mission or period of working operation is increased.

Perfect and worst case fault detection are found to provide the highest rate of information transmission, while poor or noisy fault detection has a zero transmission rate. The Bayes criterion allows a higher information rate than the Neyman-Pearson criterion due to its minimization of decision error. Higher information rates can be achieved with each level of redundancy. Although duplex fault detection has a higher transmission rate initially, duplex tests are outperformed by simplex tests beyond the MTBF due to their inability to distinguish between dual and single failures. Hence, a full FDI decision scheme is suggested for redundant structures which incorporates any quality simplex schemes in order to improve fault tolerance.

For a redundant structure without shutdown capability, the perfect case of errorless detection with full FDI exhibits a dramatic improvement with the level of redundancy in terms of reduced error variance and a longer period of working operation due to increased fault tolerance. Single structure performance is defined by $\mathcal{H}E1$ irregardless of any simplex tests. Error variance for a perfect redundant structure is initially lower due to the averaging of working controllers and is only gradually increased upon switching to successive stages of reduced operation. The relative improvement of the dual structure over the single structure is dependent upon the quality of the simplex test. However, a triple redundant structure of near-perfect triplex and duplex detection and poor simplex detection (e.g. the TRS of Chapter 4) shows immediate improvement over single structure performance. It also found to provide lower error entropy than both of the examined passive redundancy techniques, although it does approach the performance of a fault masking scheme as the mission progresses. Fault masking shows similar promise while majority-voting is easily observed as undesirable. Hence, a triple structure without shutdown capability can achieve significantly better performance than a single or dual structure.

For a system with zero shutdown cost and high false alarm cost, analysis of error entropy allows determination of the relative merit of redundant structures. For example, this cost analysis allows determination of whether a fault detection scheme is acceptable for even a single control structure and, if so, when during the mission it should be utilized. The perfect case of errorless detection with full FDI exhibits a dramatic improvement with the level of redundancy in terms of reduced error variance and a longer period of working operation due to increased fault tolerance. The general performance of a redundant structure with shutdown is dependent upon the quality of the tests and proper design of the decision scheme. Results indicate the need to switch the FDI decision scheme for different stages of the mission in all but the most perfect case. It is concluded that precedence for the full FDI decision scheme should agree with the most probable state for the given mission time (i.e. assume the dominant prior when designing the decision scheme). If any tests should dominate the others in quality, then only they should be utilized throughout the mission. Conversely, any tests of poor or worse quality are generally not utilized. However, a redundant structure with shutdown capability must incorporate at least one near-perfect test in order to improve upon single structure performance. The passive redundancy techniques of fault masking and majority-voting are found to be inappropriate for a system with shutdown capability.

Bibliography

1. Antsaklis, Passino, and Wang, "Autonomous Control Systems: Architecture and Fundamental Issues", Department of Electrical and Computer Engineering, University of Notre Dame, Notre Dame, IN.

2. Bazovsky, Igor, Reliability Theory and Practice, Prentice-Hall, Englewood Cliffs, NJ, 1961.

3. Bobrow, Daniel, Qualitative Reasoning About Physical Systems, MIT Press, Cambridge, MA, 1985.

4. Brockman, J., Error-Referenced Non-redundant Sample Coding for Data Conversion Systems, M.S. Thesis, University of Cincinnati, Cincinnati, OH, August, 1986.

5. Bronson, Richard, Matrix Methods, Academic Press, New York, NY, 1970.

6. Drenick, R.F., "The Failure Law of Complex Equipment", Journal of SIAM, Vol.8, p. 680, 1960.

7. Emami-Naeini, A., Akhter, M., and Rock, S., "Robust Detection, Isolation, and Accommodation for Sensor Failures", American Control Conference Proceedings, p.1129, 1985.

8. Fox, Lowenfeld, and Kleinosky, "Techniques for Sensor-Based Diagnosis", Robotics Institute, Carnegie-Mellon University, Pittsburgh, PA.

9. Gai, E., Harrison, J., and Daly, K., "Generalized Likelihood Test for FDI in Redundant Sensor Configurations", Journal of Guidance, Control, and Dynamics, Vol. 2, Jan. 1979.

10. Gai, E., Harrison, J., and Daly, K., "FDI Performance of Two Redundant Sensor Configurations", IEEE Transactions on Aerospace and Electronic Systems, Vol. AES-15, No. 3, p.405, May 1979.

11. Garrett, Patrick, Computer Interface Engineering for Real-Time Systems, Prentice-Hall, Englewood Cliffs, NJ, 1987.

12. Garrett, LeClair, and Wee, "Qualitative Process Automation vs. Quantitative Process Control", American Control Conference Proceedings, Minneapolis, MN, June 1987.

13. Garrett, Patrick, "Error Understanding in Computer Integrated Manufacturing Processes", American Control Conference Proceedings, Atlanta, GA, June 1988.

14. Gertler, Janos, "Survey of Model-Based Failure Detection and Isolation in Complex Plants", IEEE Control Systems, December, 1988, pp. 3-11.

15. Hancock, John, Signal Detection Theory, McGraw-Hill, New York, NY, 1966.

16. Horak, D.T., "Failure Detection in Dynamic Systems with Modeling Errors", Journal of Guidance, Control, and Dynamics, Vol. 11, No. 6, p. 508, Nov. 1988.

17. Jaynes, Edwin, "Where Do We Stand on Maximum Entropy?", The Maximum Entropy Formalism, edited by Raphael Levine, MIT Press, Cambridge, Massachusetts, 1979.

18. Kuo, Benjamin, Digital Control Systems, HRW, New York, NY, 1980.

19. Laube, Sam, Interpolation Error in Sampled Data Systems, Senior Project, Electrical Engineering Technology, University of Cincinnati, Cincinnati, OH, June 1983.

20. Levis, A.H., et.al., "Challenges to Control: A Collective View", IEEE Transactions on Automatic Control, Vol. AC-32, No. 4, April, 1987.

21. Matejka, Richard, A Real-Time Environment for Qualitative Process Control, Master's Thesis, Electrical and Computer Engineering, University of Cincinnati, Cincinnati, OH, June 1988.

22. Middleton, David, An Introduction to Statistical Communication Theory, McGraw-Hill, New York, NY, 1960.

23. Peebles, Peyton, Probability, Random Variables, and Random Signal Principles, 2nd Ed., McGraw-Hill, New York, NY, 1987.

24. Papoulis, Athanasios, Probability, Random Variables, and Stochastic Processes, McGraw-Hill, New York, NY, 1984.

25. Poor, Vincent, An Introduction to Signal Detection and Estimation, Springer-Verlag, New York, NY, 1988.

26. Pugachev, V.S., Theory of Random Functions and Its Application to Control Problems, Addison-Wesley Publishing Company, Reading, Mass., 1965.

27. Raemer, H.R., Statistical Communications Theory and Applications, Prentice-Hall, Englewood Cliffs, NJ, 1969.

28. Rice, S.O., "Mathematical Analysis of Random Noise", Bell System Technical Journal, Volume 23, July, 1944.

29. Saridis, George, "Toward the Realization of Intelligent Controls", Proceedings of the IEEE, Vol. 67, No. 8, August 1979.

30. Schwartz, Mischa, Information Transmission, Modulation, and Noise, 1st Ed., McGraw-Hill, New York, NY, 1959.

31. Schwartz, Mischa and Shaw, Leonard, Signal Processing: Discrete Spectral Analysis, Detection, and Estimation, McGraw-Hill, New York, NY, 1975.

32. Shanmugam, K.Sam, Digital and Analog Communication Systems, John Wiley & Sons, New York, NY, 1979.

33. Shannon, Claude E. and Weaver, Warren, The Mathematical Theory of Communication, University of Illinois Press, Urbana, Illinois, 1949.

34. Tholman, R.C., Principles of Statistical Mechanics, Oxford, Clarendon, 1938.

35. Thorman, Phillip, Measurement Instrumentation and Temperature Control Optimization for Molecular Beam Epitaxy Machine, Master's Thesis, Electrical and Computer Engineering, Unversity of Cincinnati, Cincinnati, OH, June 1989.

36. Tribus, Myron, "Information Theory as the Basis for Thermostatics and Thermodynamics", Journal of Applied Mech., Volume 28, March, 1961.

37. Valavanis, Kimon, A Mathematical Formulation for the Analytical Design of Intelligent Machines, Doctoral Dissertation, Department of Computer and Systems Engineering, Rensselaer Polytechnic Institute, Troy, NY, October 1986.

38. Van Trees, Harry, Detection, Estimation, and Modulation Theory, John Wiley & Sons, New York, NY, 1968.

39. Walker, Bruce, et.al., Fault-Tolerant Control Systems, Department of Aerospace Engineering, University of Cincinnati, Cincinnati, OH, to be published.

40. Walpole, Ronald and Myers, Raymond, Probability and Statistics for Engineers and Scientists, MacMillan Publishing, New York, NY, 1985.

41. Weber, Charles, Elements of Detection and Signal Design, Springer-Verlag, New York, NY, 1987.

42. Weidemann, Henry, "Entropy Analysis of Feedback Control Systems", pp.225-255, in Advances in Control Systems, vol. 7, edited by C.T. Leondes, Academic Press, New York, NY, 1969.

43. Wiener, Norbert, Cybernetics, M.I.T. Press, Cambridge, MA, 1961.

44. Whalen, Anthony, Detection of Signals in Noise, Academic Press, New York, NY, 1971.

45. Woodward, P.M., Probability and Information Theory With Applications to Radar, Pergamon, London, 1953.

APPENDIX A

Example Error Analysis of a Control Structure

System Element	Error (%FS)
Sensor linearization	0.0111
Cold junction compensation	0.0222
Input RC filter	0.0001
Signal quality	0.2370
OP-07 amplifier	0.0370
CMOS multiplexer	0.0110
A/D converter	0.0066
Intersample	0.0319
Sinc	0.0150
Aliasing	0.2205
Mean values	0.0484
RSS values	0.3276
Existing measurement error bound	0.3760 %FS (6.77 °C)

Note: In addition to the above repeatability errors associated with the temperature measurement, Omega Engineering documents the limits of error of the Type-C Hoskins thermocouple from true temperature.

Temperature Range	Limits of Error
0 - 425 °C	± 4.5 °C of true temperature
425 - 2320 °C	± 1 % of the reading

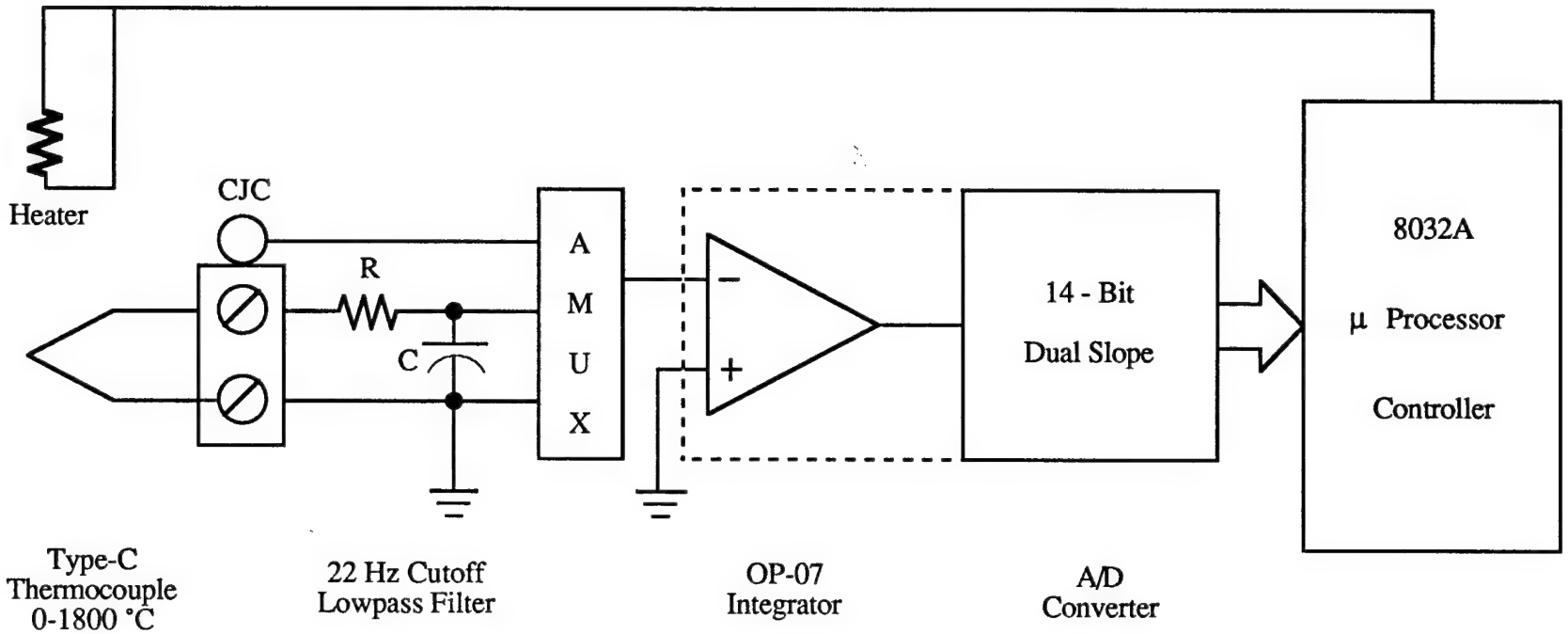


Figure A.1
Process Control Structure

Input Parameters

Input V_s = 0-31 mV from 0°C - 1800°C

Type C thermocouple, $R_s = 100\ \Omega$

Sampled at f_s = 3.75 Hz

$$\text{Signal BW} = \frac{dV_s}{dt}\ \frac{1}{\pi \cdot V_{FS_{in}}} \tag{1}$$

$$= \frac{20°C}{60\ \text{sec}}\ \frac{0.016\ \text{mV}}{°C}\ \frac{1}{\pi\ .\ 31\ \text{mV}}$$

$$= 0.05\ \text{Hz}$$

$$V_{noise_{in}} = 190\ \text{mV}_{pp}\ (67.2\ \text{mV}_{rms})$$

at $f_{coherent}$ = 20 kHz triac gate oscillator

$$\text{Input SNR}_{coherent} = \left(\frac{V_{FS_{in}}}{V_{noise_{in}}}\right)^2 \tag{2}$$

$$= \left(\frac{31\ \text{mV}}{67.2\ \text{mV}}\right)^2$$

$$= 0.213\ \text{numerical}$$

Sensor

$$\text{Linearization error} = \frac{0.2°C\ \text{rated}}{1800°C\ \text{FS}} \cdot 100\ \% \tag{3}$$

$$= \overline{0.0111}\ \%\text{FS}$$

$$\text{CJC error} = \frac{0.4°C\ \text{rated}}{1800°C} \cdot 100\ \% \tag{4}$$

$$= \overline{0.022}\ \%\text{FS}$$

Input RC Filter

$$\text{Filter error} = \frac{f_c}{10f} \sum_{0}^{\frac{10f}{f_c}} [\, 1.0 - A(f) \,] \cdot 100\% \qquad (5)$$

$$= \overline{0.0001}\ \%FS$$

$$\text{where } A(f) = \frac{1}{\sqrt{1 + (\frac{f}{f_c})^2}} \qquad (6)$$

$$\text{and } f_c = \frac{1}{2\pi RC} = 21.9 \text{ Hz. input RC filter (RC = 7.27 ms)} \qquad (7)$$

BASIC Program to Compute Filter Error

```
100 SUM = 0
110 BW = 0.05
120 FC = 21.922
130 FOR I = 1 TO 10
140    X = 1 - (1/(SQR(1+(I*BW/(10*FC))^2)))
150    SUM = SUM + X
160 NEXT I
170 SUM = (SUM/10) * 100
180 PRINT "Average Filter Error = ";SUM;" %FS"
```

Output of Program

Average Filter Error = 1.013279E-04 %FS

Signal Quality

$$\text{Filter SNR}_{\text{coherent}} = \text{Input}_{\text{SNR}} \cdot [1 + (\frac{f_{coh}}{f_c})^2] \qquad (8)$$

$$= (0.213) \cdot [1 + (\frac{20 \text{ kHz}}{21.9 \text{ Hz}})^2]$$

$$= 177{,}644 \quad (1.87 \times 10^{22} \text{ prefiltered})$$

$$\text{Amplitude Error} = \frac{100\ \%}{\sqrt{\text{SNR}_{\text{coherent}}}} \qquad (9)$$

$$= 0.237\ \%FS \quad (1 \times 10^{-9}\ \%FS \text{ prefiltered})$$

Combined Internal Noise

$$V_t = \sqrt{4kTR_s} \cdot \frac{V_{rms}}{\sqrt{Hz}} \quad (10)$$

$$= \sqrt{(4)\left(\frac{1.38 \times 10^{-23}\ J}{^\circ K}\right)(293^\circ K)(100\ \Omega)}$$

$$= \frac{1.27\ nV_{rms}}{\sqrt{Hz}} \quad \text{thermal noise}$$

$$V_c = (0.57 \times 10^{-9}) \cdot R_s \sqrt{\frac{I_{bias}}{0.1\% \cdot BW}} \cdot \frac{V_{rms}}{\sqrt{Hz}} \quad (11)$$

$$= (0.57 \times 10^{-9}) \cdot (100\ \Omega) \sqrt{\frac{3 \times 10^{-9}\ A}{0.1\% \cdot BW}} \cdot \frac{V_{rms}}{\sqrt{Hz}}$$

$$= 0.1396 \frac{nV_{rms}}{\sqrt{Hz}} \quad \text{contact noise}$$

$$V_n = \frac{18\ nV_{rms}}{\sqrt{Hz}} \quad \text{OP-07 amplifier}$$

$$I_n = \frac{0.8\ pA_{rms}}{\sqrt{Hz}} \quad \text{OP-07 amplifier}$$

$$f_{hi} = \frac{f_t}{A_v} \quad \begin{matrix}\text{Gain-Bandwidth Product of OP-07 amplifier} \\ \text{Gain of OP-07 Amplifier}\end{matrix} \quad (12)$$

where gain = Integrator period 16.67 ms/RC product 0.22 ms

$$= \frac{600\ kHz}{75.77} = 7.92\ kHz$$

$$V_{N_{rms}} = \sqrt{(V_t^2 + V_c^2) f_c + (V_n^2 + I_n^2 \cdot R_s^2) f_{hi}} \quad (13)$$

$$= \sqrt{[(1.27nV)^2+(0.139nV)^2]\cdot 21.9kHz+[(18nV)^2\cdot(0.8nV)^2]\cdot 7.92kHz}$$

$$= 1.602\ \mu V$$

$$V_{N_{pp}} = V_{N_{rms}} \cdot 6.6 \frac{V_{pp}}{V_{rms}} = 10.57\ \mu V \quad (14)$$

OP-07 Amplifier

V_{os}	=	75 µV	nulled
$\frac{dV_{os}}{dT} \cdot \Delta T$	=	$\frac{0.2\ \mu V}{°C} \cdot 10°C$	2 µV
Ios • Rs	=	(0.8 nA) • (100 Ω)	0.08 µV
$V_{N_{pp}}$	=	Combined Internal Noise	10.57 µV
$f(A_v) \cdot \frac{V_{FS_{out}}}{A_v}$	=	(100 ppm) • $\frac{2.349\ V}{75.77}$	3.1 µV
$\frac{dAv}{dT} \cdot DT \cdot \frac{VFSout}{Av}$	=	(5ppm) • (10°C) • $\frac{2.349\ V}{75.77}$	1.55 µV
V_{RSS} error at input	=		11.38 µV
Amplifier error	=	$V_{RSS} \cdot \frac{A_v}{V_{FS_{out}}} \cdot 100\ \%$	0.037 %FS
$V_{FS_{out}}$	=	$V_{FS_{in}} \cdot A_v$	2.349 V

CMOS Multiplexer

Transfer error	0.010 %
Crosstalk	0.001 %
Leakage	0.001 %
Multiplexer error	0.011 %FS

14-Bit A/D Converter

Differential nonlinearity $\frac{1}{2}$ LSB	0.0030 %
Quantizing uncertainty $\frac{1}{2}$ LSB	0.0030 %
Linearity tempco $\frac{2ppm}{°C} \cdot 10°C$	0.0020 %
A/D error	0.0066 %FS

Sampling

$$\text{Intersample error} = \frac{\sqrt{2} \cdot \pi \cdot BW \cdot V_{FS_{in}}}{\sqrt{6} \cdot f_s \cdot V_{FS_{out}}} \cdot 100\ \% \qquad (15)$$

$$= \frac{\sqrt{2}\ (\pi)\ (0.05\ \text{Hz})\ (31\ \text{mV})}{\sqrt{6}\ (3.75\ \text{Hz})\ (2.349\ \text{V})} \cdot 100\ \%$$

$$= 0.0319\ \%\text{FS}$$

$$\text{Sinc error} = \frac{1}{2} \cdot \left[1 - \frac{\sin\left(\frac{\pi BW}{f_s}\right)}{\frac{\pi BW}{f_s}} \right] \cdot 100\ \% \qquad (16)$$

$$= \frac{1}{2} \cdot \left[1 - \frac{\sin\left(\frac{\pi(0.05\ \text{Hz})}{3.75\ \text{Hz}}\right)}{\frac{\pi(0.05\ \text{Hz})}{3.75\ \text{Hz}}} \right] \cdot 100\ \%$$

$$= \overline{0.015}\ \%\text{FS}$$

$$\text{Aliasing error} = \frac{V_{noise_{in}}}{V_{FS_{in}}} \frac{1}{\sqrt{1 + \left(\frac{f_{coh}}{f_c}\right)^2}} \operatorname{sinc}\left(\frac{mf_s - f_{coh}}{f_s}\right) \cdot 100\ \% \qquad (17)$$

where m = 5334, a multiple of the sampling frequency

$$= \frac{67.2\ \text{mV}}{31\ \text{mV}} \frac{1}{\sqrt{1 + \left(\frac{20\text{kHz}}{21.9\text{Hz}}\right)^2}} \operatorname{sinc}\left(\frac{20002.5\text{Hz} - 20\text{kHz}}{3.75\text{Hz}}\right)\ 100\ \%$$

$$= (2.16)\ (0.0011)\ (0.928)\ (100\ \%)$$

$$= 0.2205\ \%\text{FS} \quad (2 \times 10^{-9}\ \%\text{FS prefiltered})$$

Appendix B

System Entropy of Redundant Structures

With Respect to the Failure Time and Conditional Error Functions

This exercise is presented as a traditional analysis of the uncertainty inherent within continuous distributions. A single and dual redundant control structure are reviewed with respect to the failure time and conditional error functions for a given mission length T. The measure function of Section 5.4 is included in order to provide a common basis for uncertainty comparisons. It is found that structure entropy is increased with mission time T and level of redundancy N. These results are concerned with the uncertainty of the exact time of failure (i.e. the failure time function), but this is not typically a decision that is made. A more relaxed decision is traditionally made regarding structure (un)reliability for a given time t of the process or mission. Section 5.6 provides a system entropy analysis for these more commonly made decisions with respect to the reliability distribution.

A joint or system entropy $\mathcal{H}_{system}(T)$, which represents all a priori uncertainty inherent within a control structure for a given mission time T, can be formulated directly from the entropy of the failure time density function f(t) for the structure and the mean conditional entropy of the error function with respect to the structure failure time t_f (as per Equation 5.12c).

$$\mathcal{H}_{system}(T) = \mathcal{H}(\varepsilon, f \mid T) = \mathcal{H}(f \mid T) + \mathcal{H}(\varepsilon \mid f, T)$$

A common measure function for the conditioned error and failure time density functions of the DDRS is needed to define the zero position on the entropy scale in order to facilitate uncertainty comparisons and formulation of a joint or system entropy. Intrinsically, zero entropy represents the most certain or accurate distribution. A uniform measure function $m(x) = 1/\Delta_x$ with Δ_x arbitrarily chosen to be 0.001%FS (representing an accuracy of $\pm$ 0.0005%FS) is defined to be the most certain or accurate distribution. It is standard

engineering practice that 5 orders of magnitude difference can be considered relatively unmeasurable or zero. Fullscale value for the failure time density function shall be the mission time T, with a default value of $T = \infty$ unless otherwise specified. The entropy relative to this common measure function is determined by Equation 5.9 for the conditioned error and failure time density functions is as follows:

$$\mathcal{H}(\varepsilon | \text{ Both Structures Working}) = \log\left(\frac{\sigma\sqrt{2\pi e}}{0.001\%FS\sqrt{2}}\right)$$

$$\mathcal{H}(\varepsilon | \text{ Single Structure Working}) = \log\left(\frac{\sigma\sqrt{2\pi e}}{0.001\%FS}\right)$$

$$\mathcal{H}(\varepsilon) = \mathcal{H}(\varepsilon | \text{ Neither Structure Working}) = \log\left(\frac{200\%FS}{0.001\%FS}\right) = 12.2$$

$$\mathcal{H}(f \mid T) = -\int_0^T f(t) \log\frac{f(t)}{m(t)}\,\partial t = -\int_0^T \lambda \exp(-\lambda t) \log\left(\frac{\lambda \exp(-\lambda t)}{0.00001 * T}\right)\partial t$$

$$= (\log(\lambda) - \lambda T - 1)\exp(-\lambda T) + \log\left(\frac{e\,10^5}{\lambda T}\right)$$

All of the above equations assume independence of the two structures. Note that the entropy is dimensionless within the logarithm due to the measure function. The first two equations are derived directly from Shannon's entropy for a Gaussian distribution (Equation 5.3) with application of the change in error deviation for redundant structures (Equation 3.3). The third equation assumes a uniform conditioned error distribution over all possible values (± 100%FS) and is derived directly from Shannon's entropy for uniform distributions (Equation 5.2). This equation also represents the error distribution entropy with no knowledge of the working states of the dual structures. The last equation defines entropy for the failure time density function (Equation 3.6) and the given mission time T. It is derived directly from Shannon's entropy for exponential distributions

(Equation 5.4). As the mission time approaches $+\infty$, $\mathfrak{H}(f|T) = \mathfrak{H}(f)$ approaches $-\infty$ (i.e. absolute certainty in the failure time relative to the total mission time).

The mean conditional entropy $\mathfrak{H}(\varepsilon|f,T)$ of the error function $\varepsilon(x)$ (Equation 5.17) is defined as the uncertainty of the error for a given failure time t_f and averaged over the mission time T with respect to the failure time function f(t) (as per Equation 5.15c). The probability of the error for a given failure time can be defined from the component probabilities of the error conditioned upon the reliability R(t) and unreliability Q(t) of the control structure. The entropy of the error conditioned upon the reliability (Structure Working) and unreliability (Structure Not Working) was derived above.

$$\mathfrak{H}(\varepsilon|f,T) = -\int_0^T f(t) \int_{-FS}^{FS} \mathcal{E}(x|t,t_f) \log \frac{\mathcal{E}(x|t,t_f)}{m(x)} \, \partial x \, \partial t$$

$$\mathcal{E}(x|t,t_f) = p(\varepsilon = x|t,t_f) = p(\varepsilon = x|t < t_f)\, p(t < t_f) + p(\varepsilon = x|t \geq t_f)\, p(t \geq t_f)$$

$$= \text{Gaussian}(0,\sigma) \times R_S(t) + \frac{1}{200\%FS} \times Q_S(t)$$

$$\mathfrak{H}(\varepsilon|f,T) = -\int_0^T f(t)\, R_S(t) \int_{-FS}^{FS} \text{Gaussian}(0,\sigma) \log \frac{\text{Gaussian}(0,\sigma)}{m(x)} \, \partial x +$$

$$f(t)\, Q_S(t) \int_{-FS}^{FS} \frac{1}{200\%FS} \log \frac{1}{200\%FS\, m(x)} \, \partial x \, \partial t$$

$$\mathfrak{H}(\varepsilon|f,T) = \int_0^T f(t)\, R_S(t)\, \mathfrak{H}(\varepsilon|\text{Structure Working}) + f(t)\, Q_S(t)\, \mathfrak{H}(\varepsilon|\text{Structure Not Working}) \, \partial t$$

$$\mathfrak{H}(\varepsilon|f,T) = \log\left(\frac{\sigma\sqrt{2\pi e}}{0.001\%FS}\right) \int_0^T \lambda \exp(-2\lambda t) \, \partial t +$$

$$\log\left(\frac{200\%FS}{0.001\%FS}\right) \int_0^T \lambda \left(\exp(-\lambda t) - \exp(-2\lambda t)\right) \partial t$$

$$\mathcal{H}(\varepsilon|\, f,T) \;=\; \frac{1}{2}\log\left(\frac{\sigma\sqrt{2\pi e}}{200\%FS}\right)(1-\exp(-2\lambda T)) \;+\; 12.2\,(1-\exp(-\lambda T))$$

Note that the mean conditional entropy is less than the unconditioned entropy for all T.

$$\mathcal{H}(\varepsilon|\, f,T) \;<\; \mathcal{H}(\varepsilon) \;=\; 12.2$$

Similarly, a joint or system entropy $\mathcal{H}_{system}(T)$, which represents all a priori uncertainty inherent within the DDRS for a given mission time T, can be formulated directly from the entropy of the failure time density functions $f_1(t)$ and $f_2(t)$ for the two redundant structures and the mean conditional entropy of the error function with respect to the structure failure times t_{f1} and t_{f2}. All entropy is formulated with respect to an arbitrary measure function m(x) in order to define a common zero point on the entropy scale (Equation 5.9).

$$\mathcal{H}_{system}(T) \;=\; \mathcal{H}(\varepsilon,f_1,f_2\,|T) \;=\; \mathcal{H}(f_1\,|T) \;+\; \mathcal{H}(f_2\,|f_1,T) \;+\; \mathcal{H}(\varepsilon\,|f_1,f_2,T)$$

The uncertainty $\mathcal{H}(f_2\,|f_1,T)$ of the failure time function $f_2(t)$ for the second control structure over a given mission time T conditioned on the knowledge of the failure time t_{f1} for the first structure is equivalent to the unconditioned entropy of the failure time since the performance of the two structures is independent.

$$\mathcal{H}(f_2\,|f_1,T) \;=\; \mathcal{H}(f_1\,|T) \;=\; (\log(\lambda) - \lambda T - 1)\exp(-\lambda T) + \log\left(\frac{e\,10^5}{\lambda T}\right)$$

This increase in system entropy is replicated (linearly proportional) with each additional level of redundancy. The mean conditional entropy $\mathcal{H}(\varepsilon\,|f_1,f_2,T)$ of the error function $\varepsilon(x)$ is defined by its component entropies which are further conditioned upon the state of the system: both structures working, single structure working, neither structure working.

$$\mathcal{H}(\varepsilon|\, f_1,f_2,T) = -\int_0^T\int_0^T f(t_1)\, f(t_2) \int_{-FS}^{FS} \mathcal{E}(x|\, t,t_{f1},t_{f2}) \log \frac{\mathcal{E}(x|\, t,t_{f1},t_{f2})}{m(x)}\, \partial x\, \partial t_2\, \partial t_1$$

$$\mathcal{E}(x|\, t,t_{f1},t_{f2}) = p(\varepsilon = x|\, t < t_{f1},\, t < t_{f2})\, p(t < t_{f1},\, t < t_{f2}) +$$

$$p(\varepsilon = x|\, t < t_{f1},\, t \geq t_{f2})\, p(t < t_{f1},\, t \geq t_{f2}) +$$

$$p(\varepsilon = x|\, t \geq t_{f1},\, t < t_{f2})\, p(t \geq t_{f1},\, t < t_{f2}) +$$

$$p(\varepsilon = x|\, t \geq t_{f1},\, t \geq t_{f2})\, p(t \geq t_{f1},\, t \geq t_{f2})$$

$$\mathcal{E}(x|\, t,t_{f1},t_{f2}) = \text{Gaussian}\left(0, \frac{\sigma}{\sqrt{2}}\right) \times R_S^2(t) + \text{Gaussian}\,(0,\sigma) \times 2\, R_S(t)\, Q_S(t) + \frac{1}{200\%FS} \times Q_S^2(t)$$

$$\mathcal{H}(\varepsilon|\, f_1,f_2,T) = \int_0^T\int_0^T f(t_1)\, f(t_2) \times \Big[R_S(t_1)\, R_S(t_2)\, \mathcal{H}(\varepsilon|\, \text{Both Structures Working}) +$$

$$\big(R_S(t_1)\, Q_S(t_2) + Q_S(t_1)\, R_S(t_2)\big)\, \mathcal{H}(\varepsilon|\, \text{Single Structure Working} +$$

$$Q_S(t_1)\, Q_S(t_2)\, \mathcal{H}(\varepsilon|\, \text{Neither Structure Working})\Big]\, \partial t_2\, \partial t_1$$

$$\mathcal{H}(\varepsilon|\, f_1,f_2,T) = \int_0^T\int_0^T \lambda^2 \exp(-\lambda t_1) \exp(-\lambda t_2) \times \Big[R_S(t_1)\, R_S(t_2) \log \frac{200\%FS}{0.001\%FS\sqrt{2}} +$$

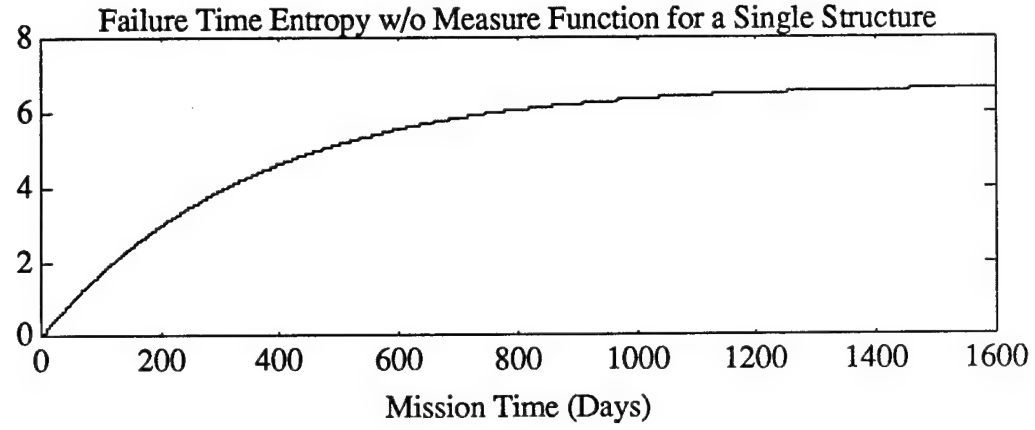
$$\big(R_S(t_1) + R_S(t_2)\big) \log \frac{\sigma\sqrt{2\pi e}}{200\%FS} + \log \frac{200\%FS}{0.001\%FS}\Big]\, \partial t_2\, \partial t_1$$

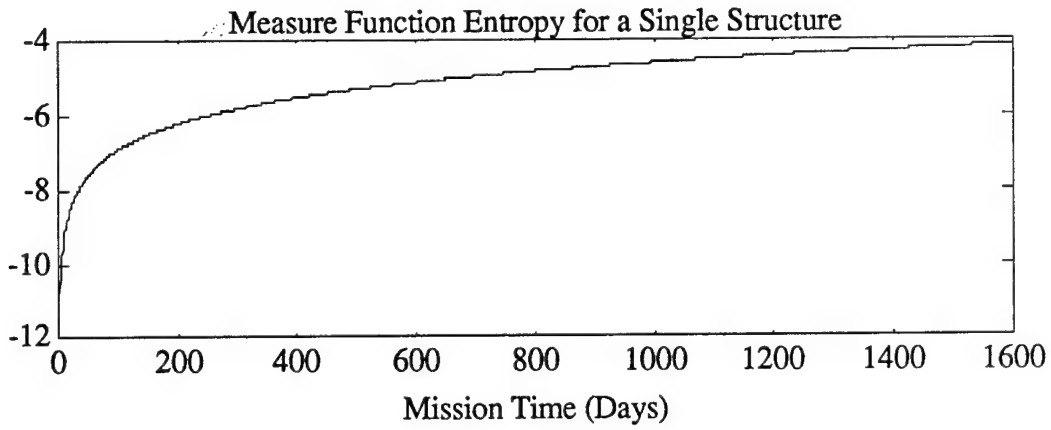
$$\mathcal{H}(\varepsilon|\, f_1,f_2,T) = 5.93\,(1 - \exp(-2\lambda T))^2 + \log\left(\frac{\sigma\sqrt{2\pi e}}{200\%FS}\right)(1 - \exp(-2\lambda T))\,(1 - \exp(-\lambda T))$$

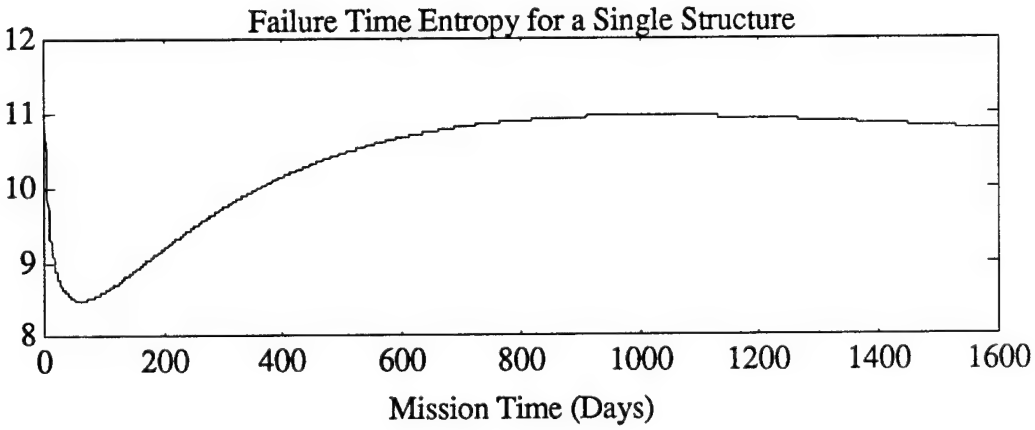
$$+ 12.2\,(1 - \exp(-\lambda T))$$

$$\mathcal{H}(\varepsilon|\, f_1,f_2,T) < \mathcal{H}(\varepsilon) = 12.2 + 5.93 = 18.13$$

The standard deviation of the example error budget (0.3276%FS, Figure 2.4) and the failure rate of the example reliability budget (0.000142, Figure 3.7) are used in producing Figures B.1 - B.5.







Figures B.1 - B.3 Failure Time Entropy

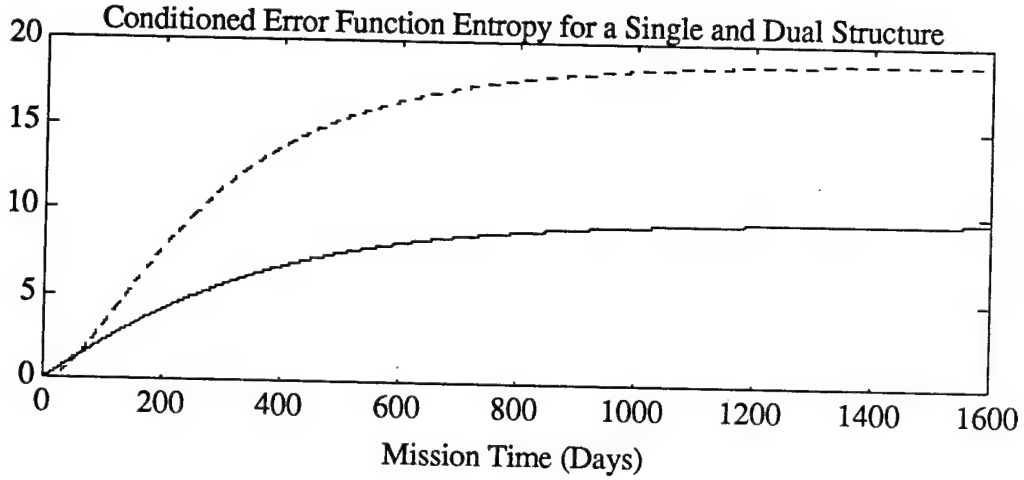


Figure B.4 Conditioned Error Entropy

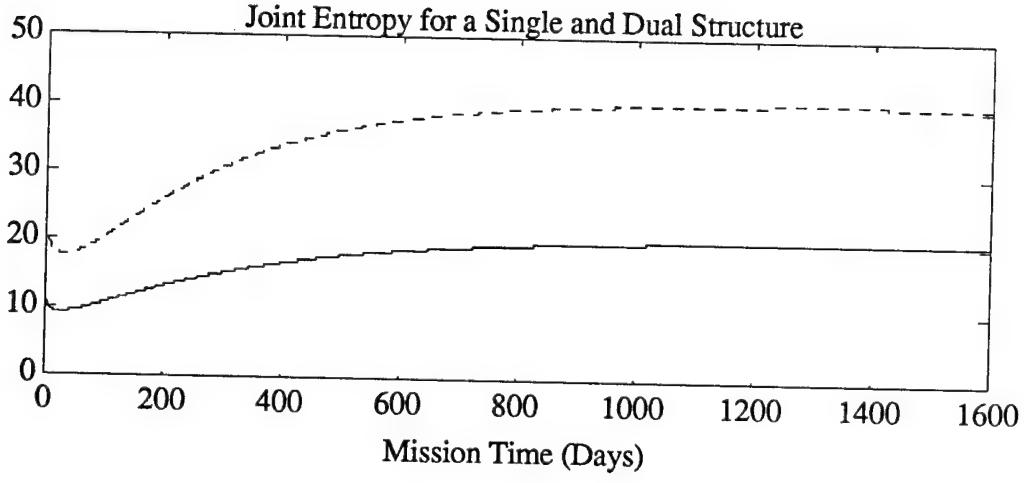


Figure B.5 Joint or System Entropy

As presented in Figures B.1 and B.4, entropy is increased for longer mission times with respect to the failure time function and the error function conditioned on the failure time. This application of entropy represents the uncertainty of the exact time of failure of each structure and of the exact amount of error given the failure time. The introduction of the measure function m(x) (Figure B.2) provides an exception for very short/long mission times where it is impossible/easy to define the exact failure time with respect to the mission time (Figure B.3). Thus, the entropy decreases with an increase in mission time for very small/long mission times. However, the time interval of interest is for mission times about the MTBF (i.e. 293 days for the example failure rate used).

As presented in Figures B.4 - B.5, entropy is also increased for an additional level of redundancy with respect to the failure time function and the error function conditioned on the failure time. This result seems reasonable since we would expect additional uncertainty with each additional structure of uncertain reliability. Due to the independence assumption for redundant structures, this increase in the failure time entropy is linearly proportional to the level of redundancy. This increase in entropy is also apparent in the conditional error function (Figure B.4) except in missions of a short period where the reduction in error variance plays a key role. Regardless, the joint or system entropy of the control structure is increased with redundancy for all mission times (Figure B.5).

The key point of this application is the use of the failure time function as the basis for the system uncertainty. However, the exact time of a structure failure is not typically a decision made for a given mission or process. The more relaxed decision of structure (un)reliability at a given time of the process (i.e. the possibility of a failure occurring before/after the given time) is the more conventional application of this knowledge. Section 5.6 provides a joint or system entropy of the control structure for a given time t based on the binary (un)reliability event set and the continuous error function conditioned upon these events.

Appendix C

Matlab Programs

```
% Calculation of Threshold T and probability of error pE
%    over time t for DDRS fault detection and isolation
%     under Bayes and Neyman-Pearson criteria

% Matlab program, Victor J. Hunt (9/91)

sigma = .3276*sqrt(2);
lamda = .000142*24;
f = 5*sigma;

for i=1:1600,      t(i) = i;

%Prior:Event 0
E0(i) = exp(-2*lamda*i);

%Threshold by Bayes criterion
%T(i) = f/2 + sigma*sigma*log(E0(i)/(1-E0(i)))/f;
%if T(i) <  0, T(i) =  0; end;
%if T(i) > 100, T(i) = 100; end;

%Threshold by NP criterion
T(i) = 3*sigma;

%Prior:Event 2
E2(i) = (.01*T(i) - T(i)^2/40000)*((1-exp(-1*lamda*i))^2);

%Conditionals
p00(i) = erf(T(i)/(sigma*sqrt(2)));
p10(i) = 1-p00(i);
p01(i) = 0.5*(erf((T(i)-f)/(sigma*sqrt(2))) - erf(-
1*(T(i)+f)/(sigma*sqrt(2))));
p11(i) = 1-p01(i);

%Prob.of Error for fault detection
pE0(i) = E0(i)*p10(i);                %false alarm
pE2(i) = E2(i)*p00(i);                %missed detection
pE1(i) = (1-E0(i)-E2(i))*p01(i);      %missed detection
pEd(i) = pE0(i)+pE1(i)+pE2(i);
```

```
%Prob.of Error for fault isolation
%pEi(i) = (1 - .02*T(i) - T(i)^2/10000)*((1-exp(-1*lamda*i))^2)*p11(i)
+ %E2(i)*p10(i) + (exp(-1*lamda*i) - E0(i))*p11(i);

%Total prob.of error
%pE(i) = pEd(i) + pEi(i);

end;


% Calculation of Threshold T and probability of error pE
%  over increasing f and time t for DDRS fault detection
%   under Bayes and Neyman-Pearson criteria

% Matlab program, Victor J. Hunt (9/91)

sigma = .3276*sqrt(2);
lamda = .000142*24;

for j=1:10                          % Ten different f magnitudes
f = 0.5*j*sigma;

%Threshold & Conditionals for NP criterion (constant)
T = 3*sigma;
p00 = erf(T/(sigma*sqrt(2)));
p01 = 0.5*(erf((T-f)/(sigma*sqrt(2))) - erf(-1*(T+f)/(sigma*sqrt(2))));
p10 = 1 - p00;
p11 = 1 - p01;

for i=1:1600                        % Mission length = 1600 days

%Prior: Event 0
E0 = exp(-2*lamda*i);

%Threshold for Bayes criterion
%T(j,i) = f/2 + sigma*sigma*log(E0/(1-E0))/f;
%if T(j,i) <  0, T(j,i) =  0; end;
%if T(j,i) > 100, T(j,i) = 100; end;

E2 = (.01*T - T^2/40000)*((1-exp(-1*lamda*i))^2);
```

```
%Conditionals for Bayes criterion
%p00 = erf(T(j,i)/(sigma*sqrt(2)));
%p01 = 0.5*(erf((T(j,i)-f)/(sigma*sqrt(2))) - %erf(-
1*(T(j,i)+f)/(sigma*sqrt(2))));
%p10 = 1 - p00;
%p11 = 1 - p01;

%Prob.of Error
pE(j,i) = E0*p10 + E2*p00 + (1-E0-E2)*p01;

end;
end;


% Calculation of two estimates (T1,T2) for Circular Threshold T
%    and probability of error pE over time t for TRS fault
%    detection under Bayes criteria

% Matlab program, Victor J. Hunt (9/91)

sigma = .3276;
lamda = .000142*24;
f = 5*sigma*sqrt(2);
F = f*sqrt(2/3);

for i=1:1600,      t(i) = i;

%Prior:Event 0
E0 = exp(-3*lamda*i);  r  = exp(-lamda*i);

%Two Threshold estimates under Bayes criterion
T1(i) = sqrt(F*F/2 + sigma*sigma*log(E0/(1-E0)));
T22 = F*F/2 + (sigma*sigma*6/f/f + 2)*sigma*sigma*log(E0/(1-E0));

if T22 < 0, T2(i) = 0;
else T2(i) = sqrt(T22);
end;

%Prior:Event 2
E21 = 9*T1(i)^2/80000*(3*r*(1-r)^2);
E22 = 9*T2(i)^2/80000*(3*r*(1-r)^2);
```

```
%Prior:Event 3
E31 = 0.536*T1(i)*T1(i)^2/1000000*((1-r)*(1-r)^2);
E32 = 0.536*T2(i)*T2(i)^2/1000000*((1-r)*(1-r)^2);

%Conditionals
p101(i) = exp(-1*T1(i)^2/2/sigma/sigma);
p011(i) = 0.5*(erf((T1(i)-F)/(sigma*sqrt(2))) - erf(-
1*(T1(i)+F)/(sigma*sqrt(2))));

p102(i) = exp(-1*T2(i)^2/2/sigma/sigma);
p012(i) = 0.5*(erf((T2(i)-F)/(sigma*sqrt(2))) - erf(-
1*(T2(i)+F)/(sigma*sqrt(2))));

%Prob.of Error for fault detection
pE01(i) = E0*p101(i);                          %false alarm
pE21(i) = E21*(1-p101(i));                     %missed detection
pE31(i) = E31*(1-p101(i));                     %missed detection
pE11(i) = (1-E0-E21-E31)*p011(i);              %missed detection
pEd1(i) = pE01(i)+pE11(i)+pE21(i)+pE31(i);

pE02(i) = E0*p102(i);                          %false alarm
pE22(i) = E22*(1-p102(i));                     %missed detection
pE32(i) = E32*(1-p102(i));                     %missed detection
pE12(i) = (1-E0-E22-E32)*p012(i);              %missed detection
pEd2(i) = pE02(i)+pE12(i)+pE22(i)+pE32(i);

end;


% Calculation of state HS, error HE, and total system HT
%     entropies over time for single, dual, and triple
%     redundant structures w/o FDI or reconfiguration

% Entropy measure function = Gaussian Function of the
%         Conditional Error for Operational TRS

% Matlab program, Victor J. Hunt (10/91)

e = 2.718282;
sigma = .3276;                  %Single structure error deviation
lamda = .000142*24;             %Single structure failure rate
```

```
for i=1:1600,      t(i) = i;

%Reliability and Unreliability for Single Structure
r(i) = exp(-1*lamda*i); q(i) = 1-r(i);

%Single Structure Entropy
HS1(i)  = -1*r(i)*log(r(i)) - q(i)*log(q(i));
HE1(i) =  r(i)*log(sqrt(3)) +
q(i)*log(200*sqrt(3/2)/(sigma*sqrt(pi*e)));
HT1(i)  =  HS1(i) + HE1(i);

%Dual Structure Entropy
HS2(i) =  -1*r(i)^2*log(r(i)^2) - 2*r(i)*q(i)*log(2*r(i)*q(i)) -
q(i)^2*log(q(i)^2);
HE2(i) =  r(i)^2*log(sqrt(3/2)) +
2*r(i)*q(i)*log(100*sqrt(3/2)/(sigma*sqrt(pi*e)))  +
q(i)^2*log(100/(sigma*sqrt(2)));
HT2(i) = HS2(i) + HE2(i);

%Triple Structure Entropy
HS3(i) =  -1*r(i)^3*log(r(i)^3) - 3*q(i)*r(i)^2*log(3*q(i)*r(i)^2) -
3*r(i)*q(i)^2*log(3*r(i)*q(i)^2) - q(i)^3*log(q(i)^3);
HE3(i) = 3*q(i)*r(i)^2*log(100*sqrt(2/3)/(sigma*sqrt(pi*e))) +
3*r(i)*q(i)^2*log(100*sqrt(2)/(3*sigma))  +
q(i)^3*log(100/(sigma*sqrt(3)));
HT3(i) = HS3(i) + HE3(i);

%Worst-case Conditional Error Entropy
HE(i)  =  log(200*sqrt(3/2)/(sigma*sqrt(pi*e)));

end;
end;


% Calculation of error HE entropy over time t for
%      Single structure with FDI which is: poor,
%      worst-case, and perfect-case

% Entropy measure function = Gaussian Function of the
%         Conditional Error for Operational TRS
```

```
% Matlab program, Victor J. Hunt (10/91)

lamda = .000142*24;          %Single structure failure rate

for i=1:1600,      t(i) = i;

%Reliability and Unreliability for Single Structure
r = exp(-1*lamda*i);    q = 1-r;

%Poor FDI case (pii = pij = .5)
HS2p(i) = -1*r^2*0.5*log(r^2*0.5) - q*r*log(q*r) - (r^2*0.5 +
q*r*0.5)*log(r^2*0.5 + q*r*0.5) - (q^2*0.5 + q*r*0.5)*log(q^2*0.5 +
q*r*0.5) - q^2*0.5*log(q^2*0.5);

%Cond.Error Entropy
HE2p(i) =  r^2*0.5*log(sqrt(3/2)) +
q*r*log(100*sqrt(3/2)/(sigma*sqrt(pi*e))) + (r^2*0.5 +
q*r*0.5)*log(sqrt(3)) + (q^2*0.5 +
q*r*0.5)*log(200*sqrt(3/2)/(sigma*sqrt(pi*e))) +
q^2*0.5*log(100/(sigma*sqrt(2)));

%Total Entropy
HT2p(i) = HS2p(i) + HE2p(i);

%Worst case (pii=0,pij=1)
%HS2wc(i) = HS2(i);
HS2(i) =  -1*r^2*log(r^2) - 2*r*q*log(2*r*q) - q^2*log(q^2);

%Cond.Error Entropy
HE2wc(i) =  2*q*r*log(100*sqrt(3/2)/(sigma*sqrt(pi*e))) +
r^2*log(sqrt(3)) + q^2*log(100/(sigma*sqrt(2)));

%Total Entropy
HT2wc(i) = HS2(i) + HE2wc(i);

%Perfect case
%HS2pc(i) = HS2(i);

%Cond.Error Entropy
HE2pc(i) =  r^2*log(sqrt(3/2)) + 2*q*r*log(sqrt(3)) +
q^2*log(100/(sigma*sqrt(2)));
```

```
%Total Entropy
HT2pc(i) = HS2(i) + HE2pc(i);

end;


% Calculation of error HE entropy over time t for
%       Single structure with possible shutdown and
%      with FDI which is: poor, worst-case, and
%      perfect-case

% Entropy measure function = Gaussian Function of the
%         Conditional Error for Operational TRS

% Matlab program, Victor J. Hunt (10/91)

lamda = .000142*24;                    %Single structure failure rate

for i=1:1600,      t(i) = i;

%Reliability and Unreliability for Single Structure
r = exp(-1*lamda*i);    q = 1-r;

%Poor FDI case (pii = pij = .5)
HE1p(i) =  0.5*r*0.55 + 0.5*q*5.54;

%Worst case (pii=0,pij=1)
HE1wc(i) =  q*5.54;

%Perfect FDI
HE1pc(i) =  r*0.55;

end;


% Calculation of error HE entropy over time t for
%       Single structure with possible shutdown,
%      false alarm cost = missed detection cost,
%      and with FDI which is: poor, worst-case,
%      and perfect-case
```

```
% Entropy measure function = Gaussian Function of the
%         Conditional Error for Operational TRS

% Matlab program, Victor J. Hunt (10/91)

lamda = .000142*24;                    %Single structure failure rate

for i=1:1600,      t(i) = i;

%Reliability and Unreliability for Single Structure
r = exp(-1*lamda*i);    q = 1-r;

%Poor FDI case (pii = pij = .5)
HE1p2(i) =  0.5*r*6.09 + 0.5*q*5.54;

%Worst case (pii=0,pij=1)
HE1wc2(i) =  5.54;

%Perfect FDI
HE1pc2(i) =  r*0.55;

end;


% Calculation of state HS, error HE, and total system HT
%      entropies over time t for Dual structure (DDRS)
%       with FDI under Bayes and Neyman-Pearson criteria

% Entropy measure function = Gaussian Function of the
%         Conditional Error for Operational TRS

% Matlab program, Victor J. Hunt (10/91)

e = 2.718282;
sigma = .3276;                  %Single structure error deviation
lamda = .000142*24;             %Single structure failure rate
f = 5*sigma*sqrt(2);

for i=1:1600,      t(i) = i;

%Priors
r = exp(-1*lamda*i);    q = 1-r;
```

```
%Event 0
E0 = exp(-2*lamda*t(i));

%Threshold by Bayes
T = f/2 + sigma*sigma*2*log(r^2/(1-r^2))/f;
%if T <  0, T =  0; end;
%if T > 100, T = 100; end;

%Threshold by Neyman-Pearson
%T = 3*sigma*sqrt(2);

%Priors: Dual Faults
d1 = q^2*(.01*T - T^2/40000);
d2 = q^2*(1-(.01*T - T^2/40000));

%Conditionals
p00 = erf(T/(sigma*2));
p10 = 1-p00;
p01 = 0.5*(erf((T-f)/(sigma*2)) - erf(-1*(T+f)/(sigma*2)));
p11 = 1-p01;

%Dual Structure Entropy with FDI & restructure to Single Structure

%Channel Outcome Entropy
HY2b(i) = -1*(r^2*p00 + 2*r*q*p01 + d1*p00 + d2*p01)*log(r^2*p00 +
2*r*q*p01 + d1*p00 + d2*p01) - (r^2*p10 + 2*r*q*p11 + d1*p10 +
d2*p11)*log(r^2*p10 + 2*r*q*p11 + d1*p10 + d2*p11);

%Cond. Channel Entropy
HC2b(i) = -1*r^2*(p00*log(p00) + p10*log(p10)) -
2*q*r*(p01*log(p01) + p11*log(p11)) - d1*(p00*log(p00) +
p10*log(p10)) - d2*(p11*log(p11) + p01*log(p01));

%Total Rate
RT2b(i) = HY2b(i) - HC2b(i);

%State Entropy
HS2b(i) = -1*r^2*p00*log(r^2*p00) - 2*q*r*p01*log(2*q*r*p01) -
(r^2*p10 + q*r*p11)*log(r^2*p10 + q*r*p11) - (d1*p10 + d2*p11 +
q*r*p11)*log(d1*p10 + d2*p11 + q*r*p11) - (d1*p00 +
d2*p01)*log(d1*p00 + d2*p01);
```

```
%Cond.Error Entropy
HE2b(i) =  r^2*p00*0.2 + 2*q*r*p01*4.85 + (r^2*p10 + q*r*p11)*0.55 +
(d1*p10 + d2*p11 + q*r*p11)*5.54 + (d1*p00 + d2*p01)*5.37;

%Total Entropy
HT2b(i) = HS2b(i) + HE2b(i);

end;


% Calculation of state HS, error HE, and total system HT
%      entropies over time t for Dual structure (DDRS)
%      with FDI which is: poor, worst, and perfect-case

% Entropy measure function = Gaussian Function of the
%        Conditional Error for Operational TRS

% Matlab program, Victor J. Hunt (10/91)

e = 2.718282;
sigma = .3276;                %Single structure error deviation
lamda = .000142*24;           %Single structure failure rate

for i=1:1600,      t(i) = i;

%Reliability and Unreliability for Single Structure
r = exp(-1*lamda*i);    q = 1-r;

%Poor FDI case (pii = pij = .5)
%Outcome Entropy
HY2p(i) = log(2);
%Cond. Entropy
HC2p(i) = log(2);
%State Entropy
HS2p(i) = -0.5*r^2*log(0.5*r^2) - r*q*log(r*q) - 0.5*q^2*log(0.5*q^2) -
0.5*(r^2 + r*q)*log(0.5*(r^2 + r*q)) - 0.5*(q^2 + r*q)*log(0.5*(q^2 +
r*q));
%Cond.Error Entropy
HE2p(i) = r^2*0.1 + r*q*4.85 + q^2*2.685 + (r^2 + r*q)*0.275 + (q^2 +
r*q)*2.77;
%Total Entropy
HT2p(i) = HS2p(i) + HE2p(i);
```

```
%Worst case (pii=0,pij=1)
%Outcome Entropy
HY2wc(i) = -1*r^2*log(r^2) - (2*r*q + q^2)*log(2*r*q + q^2);
%State Entropy
HS2wc(i) =  -1*r^2*log(r^2) - 2*r*q*log(2*r*q) - q^2*log(q^2);
%Cond.Error Entropy
HE2wc(i) =  r^2*0.55 + 2*r*q*4.85 + q^2*5.37;
%Total Entropy
HT2wc(i) = HS2wc(i) + HE2wc(i);

%Perfect FDI
%State Entropy
HS2pc(i) = -1*r^2*log(r^2) - r*q*log(r*q) - (r*q + q^2)*log(r*q + q^2);
%Cond.Error Entropy
HE2pc(i) = r^2*0.2 + r*q*0.55 + (r*q + q^2)*5.54;
%Total Entropy
HT2pc(i) = HS2pc(i) + HE2pc(i);

end;


% Calculation of information rate RT and error entropy HE
%      over time t for Dual structure (DDRS) with Full FDI
%       which is: poor, worst, perfect, and perfect/poor

% Entropy measure function = Gaussian Function of the
%         Conditional Error for Operational TRS

% Matlab program, Victor J. Hunt (10/91)

e = 2.718282;
sigma = .3276;                  %Single structure error deviation
lamda = .000142*24;             %Single structure failure rate

for i=1:1600,      t(i) = i;

%Reliability and Unreliability for Single Structure
r = exp(-1*lamda*i);    q = 1-r;
```

```
%Poor FDI case (pii = pij = .5)
%Cond.Error Entropy
HE2F1p(i) = r^2*0.025 + r*q*1.213 + q^2*0.671 + (r^2 + r*q)*0.481 +
(q^2 + r*q)*4.85;

%Worst case (pii=0,pij=1)
%Cond.Error Entropy
HE2F1wc(i) =  r^2*0.55 + 2*r*q*5.54 + q^2*5.37;

%Perfect FDI
%Cond.Error Entropy
HE2F1pc(i) = r^2*0.2 + 2*r*q*0.55 + q^2*5.54;

%Perfect Duplex, Poor Simplex
%Cond.Error Entropy
HE2F1pcp(i) = r^2*0.05 + (r^2*0.75 + r*q)*0.55 + (q^2 + r*q)*5.54;

%Poor Duplex, Perfect Simplex
%Rate
RT2F2ppc(i) = -1*(1-q^2)*0.5*log(1-q^2) - q^2*0.5*log(q^2);
RT2F1ppc(i) = -1*r^2*0.5*log(r^2) - (2*r*q + r^2*0.5)*log(2*r*q +
r^2*0.5) - q^2*log(q^2);
%Cond.Error Entropy
HE2F2ppc(i) = r^2*0.1 + r*q*4.85 + q^2*2.685 + (r^2 + 2*r*q)*0.275 +
q^2*2.77;
HE2F1ppc(i) = r^2*0.1 + (r^2*0.5 + 2*r*q)*0.55 + q^2*5.54;

end;


% Calculation of error entropy HE over time t for Dual
%      structure (DDRS) with Shutdown and with Full FDI
%       which is: poor, worst, perfect, and perfect/poor

% Entropy measure function = Gaussian Function of the
%         Conditional Error for Operational TRS

% Matlab program, Victor J. Hunt (10/91)

e = 2.718282;
sigma = .3276;                  %Single structure error deviation
lamda = .000142*24;             %Single structure failure rate
```

```
for i=1:1600,      t(i) = i;

%Reliability and Unreliability for Single Structure
r = exp(-1*lamda*i);    q = 1-r;

%Poor FDI case (pii = pij = .5)
%Cond.Error Entropy
HE2F0p(i) = r^2*0.2/8 + r*q*4.85/4 + q^2*5.37/8 + (r^2*3/4 +
r*q*11/16)*0.55 + (q^2*6/8 + r*q*17/16 + r^2/8)*5.54;
HE2F1p(i) = r^2*0.2/8 + r*q*4.85/4 + q^2*5.37/8 + (r^2 +
r*q)*0.55*5/8 + (q^2*5 + r*q*9 + r^2*2)*5.54/8;
HE2F2p(i) = r^2*0.2/2 + r*q*4.85 + q^2*5.37/2 + (r^2 + r*q)*0.55*3/8 +
(q^2*3 + r*q*5 + r^2)*5.54/8;
HE2F3p(i) = (2*r*q + r^2)*5.54;

%Worst case (pii=0,pij=1)
%Cond.Error Entropy
HE2F1wc(i) =  (r^2 + 2*r*q)*5.54 + q^2*5.37;
HE2F2wc(i) =  r^2*5.54 + 2*r*q*4.85 + q^2*5.37;

%Perfect FDI
%Cond.Error Entropy
HE2F1pc(i) = r^2*0.2 + 2*r*q*0.55;

%Perfect Duplex, Poor Simplex
%Cond.Error Entropy
HE2F1pcp(i) = r^2*0.2/4 + (r^2*2 + r*q*3)*0.55/4 + (q^2*3 + r*q*5
+r^2)*5.54/4;
HE2F2pcp(i) = r^2*0.2 + r*q*6*0.55/8 + (q^2*3 + r*q*5)*5.54/4;
HE2F3pcp(i) = r^2*0.2 + 2*r*q*5.54;

%Poor Duplex, Perfect Simplex
%Cond.Error Entropy
HE2F1ppc(i) = r^2*0.1 + (r^2*0.5 + 2*r*q)*0.55;
HE2F2ppc(i) = r^2*0.1 + r*q*4.85 + q^2*5.37/2 + (r^2 + 2*r*q)*0.55/2;

end;


% Calculation of error entropy HE and total system rate RT
%       over time t for Triple Redundant Structure (TRS) with
%       masking, averaging, and ideal FDI
```

```
% Entropy measure function = Gaussian Function of the
%         Conditional Error for Operational TRS

% Matlab program, Victor J. Hunt (10/91)

lamda = .0001f42*24;              %Single structure failure rate

for i=1:1600,      t(i) = i;

%Priors
r = exp(-1*lamda*i);    q = 1-r;

%Voting or Averaging Scheme (no decisions made)
%Cond.Error Entropy
HE3v(i) =  3*q*r^2*4.45 + 3*r*q^2*4.97 + q^3*5.17;

%Fault Masking Scheme (no decisions made)
%Cond.Error Entropy
HE3m(i) =  (r^3 + 3*q*r^2 + r*q^2)*0.55 + (2*r*q^2 + q^3)*5.54;

%Perfect TRS, Poor Simplex
%Information Rate
RT3pcp(i) = -1*r^3*log(r^3) - 3*q*r^2*log(3*q*r^2) - (3*r*q^2 +
q^3)*log(3*r*q^2 + q^3);
%Cond.Error Entropy
HE3pcp(i)  = 3*q*r^2*0.2 + r*q^2*0.55 + (2*r*q^2 + q^3)*5.54;
%Cond.Error Entropy with No Cost for Shutdown
HE3pcp2(i) = 3*q*r^2*0.2 + r*q^2*0.413 + (9*r*q^2 + 3*q^3)*1.39;

%Perfect Full FDI
%Information Rate
%RT3pc(i) = HS3(i);
%Cond.Error Entropy
HE3pc(i) =  3*q*r^2*0.20 + 3*r*q^2*0.55 + q^3*5.54;
%Cond.Error Entropy with No Cost for Shutdown
HE3pc2(i) = 3*q*r^2*0.20 + 3*r*q^2*0.55;

%Perfect TRS, No Simplex
%Cond.Error Entropy with No Cost for Shutdown
HE3NS(i) = 3*q*r^2*0.20 + 3*r*q^2*5.54;

end;
```